(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 August 2001 (30.08.2001)

PCT

(10) International Publication Number
WO 01/63528 A1

(51) International Patent Classification[7]: G06F 17/60

(21) International Application Number: PCT/US01/05706

(22) International Filing Date: 22 February 2001 (22.02.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/511,537 23 February 2000 (23.02.2000) US

(71) Applicant *(for all designated States except US)*: IPDN CORPORATION [US/US]; 104 E. Main Street. DuQuoin. IL 62832 (US).

(72) Inventors: and

(75) Inventors/Applicants *(for US only)*: SAIGH, Michael, M. [US/US]; 535 East Main Street. DuQuoin. IL 62832 (US). BARRETTE, Pierre, Philip [US/US]; 662 Lake Shore Drive. Murphysboro. IL 62966 (US).

(74) Agents: BEULICK, John, S. et al.; Armstrong Teasdale LLP. Suite 2600, One Metropolitan Square. St. Louis. MO 63102 (US).

(81) Designated States *(national)*: AE. AG. AL. AM. AT. AU. AZ, BA. BB. BG. BR. BY. BZ. CA. CH. CN. CR. CU. CZ. DE. DK. DM. DZ. EE. ES. FI. GB. GD. GE. GH. GM. HR. HU. ID. IL. IN. IS. JP. KE. KG. KP. KR. KZ. LC. LK. LR. LS. LT. LU. LV. MA. MD. MG. MK. MN. MW. MX. MZ. NO. NZ. PL. PT. RO. RU. SD. SE. SG. SI. SK. SL. TJ. TM. TR. TT. TZ. UA. UG. US. UZ. VN. YU. ZA. ZW.

(84) Designated States *(regional)*: ARIPO patent (GH. GM. KE. LS. MW. MZ. SD. SL. SZ. TZ. UG. ZW). Eurasian patent (AM. AZ. BY. KG. KZ. MD. RU. TJ. TM). European patent (AT. BE. CH. CY. DE. DK. ES. FI. FR. GB. GR. IE. IT. LU. MC. NL. PT. SE. TR). OAPI patent (BF. BJ. CF. CG. CI. CM. GA. GN. GW. ML. MR. NE. SN. TD. TG).

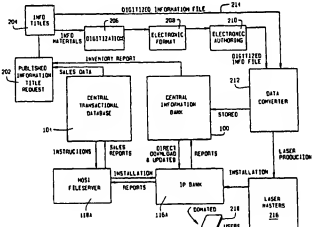
Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

[Continued on next page]

(54) Title: METHODS AND DEVICES FOR STORING, DISTRIBUTING, AND ACCESSING INTELLECTUAL PROPERTY IN DIGITAL FORM



(57) Abstract: In one embodiment, the present invention is an apparatus for facilitating obtaining text of an IP, the apparatus including a storage device (116A) having stored therein text of a plurality of IP, wherein the text includes electronically stored representations of printed text works, movies, films, video presentations, television programming, music, audio works, audio presentations, radio programs, graphic material, art works, plays, operas, novels, writings, photographs, pictures, images (including electronic images of all types including virtual images), advertising copy, or software, or portions and combinations thereof; a processor (118A) connected to the storage device (116A), the storage device (116A) further having stored therein a program for controlling the processor to: receive an IP selection request; receive a user identification associated with the IP selection request; and output encrypted text of the selected IP if the user identification and IP selection are valid utilizing a determined level of IP encryption.

WO 01/63528 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHODS AND DEVICES FOR STORING, DISTRIBUTING, AND ACCESSING INTELLECTUAL PROPERTY IN DIGITAL FORM

CROSS REFERENCE TO RELATED APPLICATIONS

This application is a continuation-in-part of U.S. patent application serial no. 09/175,559, filed October 20, 1998, which is a continuation-in-part of U.S. patent application serial no. 09/049,321, filed March 27, 1998, which is a continuation of U.S. patent application serial no. 08/687,292, filed July 25, 1996 (now U.S. Patent No. 5,734,823, issued March 31, 1998), which is a continuation of U.S. patent application serial no. 08/367,056, filed December 30, 1994 (now abandoned), which is a continuation-in-part of U.S. patent application serial no. 08/296,120, filed August 25, 1994 (now abandoned), which is a continuation of U.S. patent application serial no. 07/787,536, filed November 4, 1991 (now abandoned), all of which are incorporated herein by reference.

BACKGROUND OF THE INVENTION

The present invention relates to methods and apparatus for the secure consolidated electronic storage and distribution of Intellectual Property in digital form and more particularly to methods and apparatus for electronically storing and transmitting information in consolidated, digital form to and from centralized storage facilities and users.

As used herein, "Intellectual Property" ("IP") refers to that, which in non-electronic form, would be referred to as books, text, pictures, photographs, videos, movies, films, audio, music, software, computer games, video games, and other types of expressions of ideas or concepts that can be stored and distributed in digital form. IP also includes all material that is capable of being protected by copyright, as well as other materials. In some embodiments, IP's include

compilations and/or portions of one or more of the above types of works as well as the works themselves.

Current networks for dissemination of IP lack a uniform distribution system. There are, for example, several different encryption technologies providing digital security (i.e., prevention of piracy or illegal copying of IP) for different media such as books, video, software, and multi-media. Similarly, there are different network distribution systems competing with each other to provide IP with little or no compatibility between the systems as seen from the standpoint of users, publishers (i.e., content providers), or the IP itself. Each entity has its own web-site, data center, and encryption algorithm. Uniformity is lacking because many different publishers, studios, and intellectual property owners have their own information retrieval service. Present methods and systems available for electronically distributing IP are not believed to provide a sufficient level of security against unauthorized use and copying to be acceptable vehicles for the commercial distribution of IP. This fragmentation produces inefficiencies in the distribution of intellectual property. There is currently no operator of an overall distribution network capable of providing publishers assurance of IP protection and easy-to-use, efficient, inexpensive, and universal dissemination of IP. There are currently no standards available that establish a criteria for the development and operation of the infrastructure, networking and systems for the commercial electronic delivery of IP with a level of security that would be desirable to most commercial providers of IP.

Traditionally, each type of IP has had its own unique way of being provided to the consumer. Intellectual Property (hereinafter referred to as IP) have been printed on paper and in books, for example, and music has been "burned" onto CDs. Retrieval methods for obtaining IP via digital readers, MP3 music hardware players and other hardware are currently specialized for the particular forms of IP for which the reader, player or other hardware is adapted. This form of specialization further fragments the IP market into specialized content data centers and reduces efficiency in distribution while failing to provide a level of security against

redistribution and copying that would be desirable to most commercial providers of IP. In addition, a proliferation of web-sites and market access locations make it more difficult and confusing for a consumer to access the available choices in a meaningful manner. Furthermore, a lack of uniformity in methods for identifying particular digitally-formatted IP makes it more difficult to track the flow of use of IP, because multiple tracking methods must be employed to accommodate multiple methods of identification. However, information provided in each case can be reduced, ultimately, to binary information. It would therefore be desirable to provide a distribution network designed for distributing various different IP types and a distribution method that can securely deliver each of these various IP types to the consumer, while safeguarding the transmitted IP types from illegal reproduction.

Present methods for distributing IP rely upon straight-forward transfer of data without inherent security built into the transferred data files. These methods provided adequate protection before the proliferation of public networks and the Internet. However, if one person were to "crack" a security code, any or all of the IP distributed in a file would be available for unencrypted transfer for all to have and use without regard for licensing and ownership. It would therefore be desirable to provide methods and devices for securing transferred data files that avoid making the IP available for unencrypted transfer after a code is cracked. Further, it would be beneficial to provide a distribution system and mechanism that regularly and automatically updates and/or changes encryption and decryption algorithms, keys, and/or formulae applicable to each IP electronically distributed to recapture security features for any IP for which previous encryption and decryption algorithms, keys, and/or formulae have been broken or compromised, to thereby inhibit cracking or compromising of IP encryption and decryption mechanisms.

Furthermore, the present proliferation of web sites and the Internet increases the difficulty of the user in finding and accessing specific IP's. There is currently a lack of uniformity in methods of identifying particular IP in digital form. This lack of uniformity makes it more difficult to track the flow and use of IP because

multiple tracking methods are required to accommodate multiple methods of identification. Lack of uniformity in electronic storage and distribution of IP also make distribution and delivery of IP more expensive and less efficient. Moreover, users of IP are inconvenienced because they must acquire multiple devices or software programs to read many different IP data formats.

It would therefore be desirable to provide methods and apparatus for consolidating all forms of digitally distributable IP.

It would further be desirable to provide methods and apparatus that provide a consistent interface between IP organizations and content owners on the one hand, and consumers of IP on the other.

BRIEF SUMMARY OF THE INVENTION

In one embodiment, the present invention is an apparatus for facilitating obtaining text of an IP, the apparatus including a storage device having stored therein text of a plurality of IP, wherein the text includes electronically stored representations of printed text works, movies, films, video presentations, television programming, music, audio works, audio presentations, radio programs, graphic material, art works, plays, operas, novels, writings, photographs, pictures, images, advertising copy, computer games, video games, or software, or portions and combinations thereof; a processor connected to the storage device, the storage device further having stored therein a program for controlling the processor to: receive an IP selection request; receive a user identification associated with the IP selection request; and output encrypted text of the selected IP if the user identification and IP selection are valid utilizing a determined level of IP encryption.

As is explained below, the terms "text" and "IP" as used herein are to be interpreted broadly. For example, a "IP" that is a musical recording includes "text" that is audio, or more specifically, music. Other types of "IP" may include more than one type of "text."

This embodiment of the present invention consolidates various forms of digitally distributable IP and provides a consistent interface between IP organizations and content owners on the one hand, and consumers of IP on the other.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 illustrates one embodiment of the present information distribution system architecture;

Fig. 2 illustrates information flow in the system architecture shown in Fig. 1;

Fig. 3 is a block diagram illustration of a point of purchase delivery system;

Fig. 4 is a more detailed block diagram illustration of the host fileserver shown in Fig. 3;

Fig. 5 is a perspective view of an IP Bank embodiment;

Fig. 5A is an alternative IP Bank embodiment;

Fig. 5B is yet another alternative IP Bank embodiment;

Fig. 6 is a block diagram illustration of the IP Bank circuitry;

Fig. 7 is a block diagram illustration of an end user's storage medium;

Fig. 8 illustrates the information flow for the point of purchase configuration;

Fig. 9 is a block diagram illustration of certain elements of a point of rental delivery system;

Fig. 10 is a block diagram illustration of certain elements of an IP Bank subsystem;

Fig. 11 is a block diagram illustration of certain elements of a promotional delivery system; and

Fig. 12 is a flow chart illustrating the encryption process implemented in accordance with the present invention; and

Fig. 13 is another IP Bank embodiment.

Fig. 14 is a representation of a network showing, in one embodiment of the present invention, how IP from content suppliers is provided through a central data center to a user device.

Fig. 15 is a more detailed block diagram of the user device shown in Fig. 14.

Fig. 16 is a block diagram of the user device shown in Fig. 15 to which an external authentication device is attached.

DETAILED DESCRIPTION OF THE INVENTION

As used herein, the term "network" refers to any electronic interconnection between two or more electronic devices over which data is transferred, including, but not limited to, the Internet, an intranet, a land line or traditional telephone network, a cellular or wireless mobile network, a wireless microwave network, television or radio wave transmissions, a cable network, a wireless connection (for example, infrared or microwave connections), satellite, a localized land network system, induction connection using electric lines, a wireless network using lasers as the transmitting medium, any combination of any of the preceding or any other system for the transmission of data between two or more units. A "secure network" is a network employing security measures against unauthorized access to data being transmitted via the network or data stored within a memory storage area of a device connected to the secure network.

The term "IP Bank," as used herein, refers to an interface between a network and a user. Such interface may be physically located in proximity to a central information storage facility, at a location remote from a central information storage facility (for example, in a physical housing such as a kiosk located at a retail establishment), or in proximity to and directly connected to a user's computer. In one embodiment of the invention, the IP Bank is wholly or partially a virtual device generated from an interaction a software program stored on a user's computer and software located at another IP Bank or a central information storage facility. In embodiments involving a virtual device, some of the hardware necessary for operation of an IP Bank is located proximate to or within a user's computer, or proximate to or within the IP Bank or the central information storage facility, depending upon a location at which user contact is made. For example, in one embodiment, a "IP Bank" comprises memory storage, a processing unit, a keyboard, slots for credit cards, slots for storage media on which downloaded digital data such as electronic versions of printed IP texts are stored, and a printer (for bills and receipts). A virtual "IP Bank" comprises, for example, only a memory and a processor (located at, e.g., a retail establishment, a data storage center, or at a security encryption compression module. Keyboards, slots for credit cards and storage media, etc. are supplied in this embodiment by the user's device and the user's software. Although the term "IP Bank" and "text" may suggest book-type or written material based upon a reader's prior notions of the subject matter to which these terms refer, the terms are not intended to be so limited in this description. Other types of material, such as movies, music, voice, video, graphic images, natural language and other text, audio, computer games, video games computer software material, and any other type of intellectual property capable of being converted to and stored in digital form is intended to be included when the terms "IP" and "text" are used, unless otherwise specified or made clearly obvious from context. (For example, "natural language text" does not refer to video or music.) An IP Bank is a self-service, user interactive information vending device, which, in one embodiment, is a separate, stand-alone device. In another embodiment, an IP bank includes hardware and software located at a central data

storage facility and hardware and software located within or proximate to a user's computer, with both being in electronic communication via a suitable network, thereby providing operation coordinated in a manner such that the components function in the same manner as a stand-alone IP bank. In yet another embodiment, an IP bank is a device located proximate to a user's computer or a computer board located within the user's computer and which is electronically connected to the user's computer via a suitable network connection, and which is also connectable to a central information storage facility using a suitable network. In another embodiment of the present invention, for example, each IP bank contains a high capacity, local memory storage having a customized portfolio of the most demanded information products for a particular site at which the IP Bank is located. In another embodiment, each IP Bank comprises a processor, a monitor, a network connection, and one or more slots configured for insertion of a portable memory storage medium and/or a connection to a user device, for example, a portable digital assistant (PDA). Other information is transferred via a network to an IP Bank for supplemental, secondary, and less demanded purposes. A processing unit within the IP Bank and coupled to the IP Bank local memory and storage controls downloading and dynamic encryption of information.

The term "IP," as used herein, includes all different types of intellectual property that is capable of being electronically stored in digital form. The term "IP" includes traditional printed text works, movies, films, video presentations, television programming, music, audio works or presentations, radio programming, graphic material, art works, plays, operas, novels, writings, photographs, pictures, images, advertising copy, computer games, video games, computer software, any portion of combination of the above, and/or other types of intellectual property.

The term "IP file," as used herein, refers to a digital version of an IP. The description is not dependent upon the format of the stored digitized material, and is equally applicable whether the digitized material is stored using HTML, XML, Adobe PDF (portable document format), SHOCKWAVE® format (Macromedia, Inc.,

San Francisco, CA), or any other format. Where the context so indicates, the term "IP selection request" refers to a request made by a user to obtain a copy of a given IP file. The term "selected IP," as used herein, refers to a particular IP file for which a user has made a request for a copy. The term "text," as used herein, when used in connection with a selected IP or IP file, refers to the content of the digitally stored IP file under consideration. Because the term "IP" is used herein includes not only traditional printed text works, but also other types of intellectual property capable of being electronically stored in digital form, the term "text" as used herein is intended to be interpreted with equal generality so as to include the content of the "IP," whether it be traditional printed text or the content of another type of IP to which the general term "IP" is applied herein. The general applicability of various of the embodiments of the invention disclosed herein will be appreciated if it is understood, for example, that a "IP" that is a television program includes "text" that is television programming. As another example, a "IP" that is a musical recording includes "text" that is audio, or more specifically, music. Extending the analogy further, it is easily understood that one "reads" the "text" of the musical recording "IP" by playing the music via a system that converts the digitally encoded audio into sound. Some types of "IP's" may include more than one type of "text," for example, digital representations of printed text, music, and pictures. All uses herein of the terms "IP" and "text" are intended to be generalized in a similar manner, unless it is explicitly stated that such use is intended to refer only to printed text or natural language text, or the context is such that the term "text" is obviously limited thereto.

The term "user's computer" or "user's device," as used herein, refers to any electronic device performing some or all of the functions traditionally associated with a typical desktop computer, including, but not limited to, a traditional desktop computer (such as an IBM PC, a MacIntosh® (Apple Computer, Inc., Cupertino, CA) or a clone of either), a laptop computer, PDA device, wireless connecting device, Internet connecting device (e.g., WEBTV™ (WebTV Networks, Inc., Palo Alto, CA) or others), digital telephone, video gaming device, ebook, or another electronic device capable of being electronically connected with a network.

The terms "user's computer" and "user's device" do not necessarily refer to different types of units.

As used herein, the term "nonvolatile memory" refers generally to a type of memory that does not depend upon power being continuously applied to retain information. For example, static RAM, segregated hard drive, floppy disk, CD-RW, magnetic optical disk, flash memory, electronically erasable programmable read only memory (EEPROM), and WORM (write once, read many time) memories are types of nonvolatile memory. ROM (read only memory) and field programmable gate arrays are also types of nonvolatile memory that are sometimes mask-programmed. A circuit designer would be able to choose a suitable type of nonvolatile memory for use in a circuit, giving due consideration to voltage, current, data access rate, data transfer rate, physical size of the device desired, and memory density requirements, and to whether the application requires the nonvolatile memory to be field programmable, erasable, and/or reprogrammable.

Also as used herein, the term "encryption algorithm" unless otherwise stated, includes methods for encryption, keys used for encryption, and formulae used for encryption. The term "decryption algorithm," unless otherwise stated, includes methods for decryption, keys used for decryption, and formulae used for decryption. However, keys and/or formulae are sometimes explicitly mentioned along with the algorithms in the explanation to add emphasis.

In one embodiment, a user may select portions or entire contents of one or more IPs. The selected information is then combined and downloaded to the user's storage device, for example, a "cartridge." A "cartridge," "memory module," or "storage medium," as used herein, refers to any device capable of electronic storage of digitized data and which is capable of providing access thereto in a controlled manner. The terms "cartridge," "memory module," and "storage medium" are interchangeable, unless otherwise indicated by context. The terms encompass, for example, devices such as appropriately configured compact disks (CDs), DVDs

(including DVD-R, DVD-RAM and DVD-RW), flash memory cards, and removable storage devices (including floppy disks, memory chips, ZIP™ disks, and other units), where "appropriately configured" means, for example, having instructions or data recorded thereon to control access by an access device to data recorded thereon. Also included are protected segregated portions of a data storage portion of a hard disk, and any other device for the storage of data electronically in digital form and providing controlled access thereto. In one embodiment, a cartridge includes a unique identification number and a predetermined amount of memory for storing the selected information. In another embodiment, a cartridge also includes specialized software (cartridge controlling software, or "CCS") stored in nonvolatile memory, either on a separate memory chip of the cartridge, or in a segregated protected space within a general memory storage space of the cartridge. The CCS is electronically linked to the cartridge on which it is stored, and controls and regulates reading and use of encrypted and tagged data information files stored within the general memory of the cartridge. As long as any portion of encrypted data stored on the cartridge is being accessed, CCS remains functioning and regulates and controls functions that the user is permitted to perform with regard to encrypted data in question. For example, in most cases, when an encrypted data file is accessed for reading, CCS operates to restrict the ability of the user to copy the data in a decrypted form or to print data onto hard copy. CCS also restricts the user from copying any portion of the decrypted data to any data file other than a temporary file in RAM that is automatically erased when CCS stops operating as an encrypted file that is only readable using CCS operating on authorized equipment. When the user ceases accessing encrypted data files, and CCS ceases operation, just prior to closing down, CCS totally erases all record of any decrypted data and all temporary files in which such data may have been stored. Once CCS has ceased operation, the user is no longer able to access any of the temporary files generated during previous operation, as all record of such files ever existing and the content contained therein will have been permanently excised from the user's system. Thus, in connection with related application software stored within the user's device, CCS utilizes one or more of the dynamic encryption and decryption

features, a unique serial or registration number, and various data registration headers to regulate and govern any use the user makes of encrypted files and the data stored within. Without CCS operating, a user is unable to gain access to the encrypted data. In one embodiment of the invention, CCS contains monitoring features that prevent operation of CSS should any attempt be made to alter its operation. In one embodiment, when CCS becomes inoperable for any reason, the user of the device has to bring the affected cartridge to an authorized agent for repair or replacement.

In one exemplary embodiment of CCS, CCS finds the information necessary to decrypt an encrypted text. While the user device in which CCS resides is operating, CCS restricts what the user device is capable of doing. For example, it restricts the user device so that it cannot write information to an external storage device while an internal storage device having an encrypted text is being used. When a cartridge is disengaged from the user device by removal, CCS shuts downs the user device, for example, either by shutting down its program or by operating an electronic switch to remove power from the user device. CCS also removes all temporary files related to the program from the user device. In addition, CCS reads a secure real-time clock in the user device to determine whether the user device is presently authorized to access data on a cartridge. CCS also registers when tampering occurs, such as a change in the real-time clock data caused by an obvious backdating attempt.

One embodiment of the invention enables a user to obtain updates to any data information file he or she has acquired, by utilizing a dial-up network to dial into an IP Bank or a central data storage facility, or by using the Internet to access an IP Bank or a central data storage facility through an appropriate link via a web site, or the use of a wireless network (e.g., digital satellite, cellular, wireless mobile, microwave, infrared, etc.) to gain access to an IP Bank or the central data storage facility over any network or connection. In one embodiment, a Secure Universal Resource Locator (SURL) is used, including both a secure phone number as well as an Internet-based URL. The same restrictions apply to obtaining an update as to acquire the data information file being updated.

The following sections provide a brief overview of one embodiment and a detailed description of its architecture. Following the detailed architecture description is a detailed description of point of sale delivery embodiment configurations. A detailed description of the various levels of encryption which may be used in the present system is then provided.

A. Brief Overview

In accordance with one embodiment of the present invention, information is distributed from a central information bank to a user's personalized storage medium. Information to be so distributed by the present system is received from outside sources either electronically, over various communication networks (e.g., telephone lines, cable systems, cellular systems, wireless mobile systems or other similar commercial communication networks) or from various storage mediums (e.g., magnetic or electronic disks, cartridges, or tape reels or compact disks, laser disks, tape cassettes, etc.), or in hard copy format. If information is received in a hard copy format, it is initially converted to a standard digital format (e.g., ASCII text, DOS text or other similar standard commercially available text format) by scanning or direct transcription. If information is received in a videotape, NTSC or PAL format video, then the information is digitally encoded in a ".avi" file, a Quicktime file, or other format, including the application of appropriate MPEG-X compression as needed. A content provider, i.e., an outside source, providing information can specify instructions relating to authorized use, access, and cost of the provided information that can be permanently linked to a master data file of the information when it is electronically stored or accessed. In one embodiment, instructions are electronically generated when information is received electronically. These instructions include a description of allowed uses (e.g., copy generation, printing limits and/or authorization, rental options, if any, purchase options, etc.), desired level of security against unauthorized copying or use (from level zero [virtually no security] to a maximum level [most robust security available]) and cost to a user, optionally as a function of user-selected access right. Whenever a request is made to obtain a copy of

the information file (i.e., IP File), the instructions are used in connection with the choices made by the user, within the allowed options, to generate user-specific electronic instructions for limiting use of the requested copy of the IP File. Then the information is digitized, formatted, compressed and initially encrypted to form an electronic master copy which is stored in the central information bank. The master copy is duplicated electronically and dispatched electronically through a communication network, such as a telephone or satellite network, to a point-of-sale delivery system. IP Banks form a part of such a delivery system, and the electronic copies are retained in the IP Banks for downloading into a user's personalized storage medium. Initially, a user selects the information to be downloaded and a tracking entry is made into a transactional database to record the transfer. Prior to and during downloading of the copy on the user's storage medium, the information is dynamically encrypted utilizing a varying level of encryption which is dependent upon a variety of variables, for example, an economic value of the information. A "dynamic" encryption process is utilized so that only the electronic reader associated with the user card used to access the information from the IP Bank and download the information to the user storage cartridge can be utilized to display the information in an understandable text format. In one embodiment, the "dynamic" encryption process creates, encrypts, and transmits data files, in real time, to one or more different user devices or storage media located in one or more different physical locations using a network. For example, in one embodiment, an instructor's lecture notes are electronically encrypted and transmitted in a secure manner to devices and/or storage media of students attending a lecture in real time. The notes are stored on these devices and/or storage media for current or later use.

As explained in greater detail below, in one embodiment, the dynamic encryption process uses a unique serial number (or other identification, for example, an alphanumeric or binary identification) associated with the particular user's storage medium to which the encrypted data is to be downloaded, the unique registration number given the user on registration, and the unique file number associated with the file to be downloaded, to secretly generate the encryption and decryption algorithms

and formulae to uniquely encrypt the copy of the data file as it is downloaded to the user's storage medium and to allow the user's system to decrypt the data for later reading. A copy of the algorithms and formulae are secretly stored at the central data storage facility in a portion of the memory storage having limited access. A copy of the algorithms and formula necessary to decrypt each of the acquired encrypted data files is stored in read-only form on the user's storage medium. Storage space for this read-only copy is designed so that any attempt to access the data stored thereon other than using an unaltered CSS program renders the data stored thereon unreadable. In another embodiment, instead of utilizing a unique registration number permanently tied to the storage medium being used for developing the unique encryption and decryption algorithms and formulae, a unique electronically-generated electronic number is assigned to the storage medium at the time of initial registration with the system, and that assigned number is used in developing the applicable encryption and decryption formulae and algorithms. In this embodiment, the unique electronically-generated number is a number that is randomly generated by the system and checked for uniqueness. In another embodiment, the unique electronically-generated number is generated by a system program that searches features of the user data storage medium to find a unique representation of the device, from which a unique electronic registration number is developed. In other embodiments, other methods, including combinations of these methods, are used to generate unique numbers.

In another embodiment, software programming periodically changes the applicable encryption and decryption algorithms and formulae associated with a particular encrypted IP file to provide enhanced security. In this embodiment, the changes in the applicable encryption and decryption algorithms and formulae occur when a user logs on and connects with the system through an IP Bank connected to the central information storage facility. The changes occur after expiration of a predetermined period of time from a date on which the particular encrypted IP file is initially created, or after expiration of a predetermined period of time from a date on which the applicable encryption and decryption algorithms and formulae are last changed, whichever last occurs. The periodic changing of applicable encryption and

decryption algorithms and formulae makes it more difficult for the encryption to be broken and allows recapturing of IP files into the encryption system if previous encryption has been broker. The frequency of such encryption changes is dependent upon a time value of the IP involved and a length of time that a user of the IP file in question has been authorized to access the particular encrypted IP file.

In one embodiment, security is enhanced through the use of an external authorization device affixed or linked to the reader device and a related identifier. Examples of suitable, currently-available authentication devices include parallel port software locks, iButtons™ (Dallas Semiconductor Corp., Dallas, TX), and "Smart Cards" plugged in via a pc-card.

In another embodiment of the invention, when one or more IP Banks are operated in conjunction with one or more retail establishments, each retail establishment is given a unique identification number that is used to tag each user device, user storage medium and/or encrypted IP file acquired at the retail establishment or through an IP Bank linked to the retail establishment. Using the tag information, particular user devices, storage media and/or IP files, a predetermined portion of the system revenue generated in regard to such tagged user devices, storage media and/or IP files is allocated to and shared with the retail establishment in question. In another embodiment, the tagging is further delineated to allow revenue sharing with manufacturers and distributors of user devices and/or storage media.

IP digital data transmission can occur between two or more than two mobile wireless or cellular devices. The devices can be multipurpose, for example, they may have a combination of PDA, cell phone, visual display, and/or audio capabilities. The devices transmit IP in a secure manner whether the IP is digital audio, video, text, software, or multimedia. The mobile device can also asynchronously obtain, through a wireless access portal (WAP), music, video, text, and other IP through various databases. For example, if a user wishes to access his or her favorite songs, the mobile wireless browser can be used to browse the music

database, access a music title by artist, CD title, or by some other fashion and customize the desired transfer of music IP. An actual order and payment then takes place after the user requests whether they wish to rent (and thus, autoerase) or own a copy of a requested song. A similar mechanism is used, in one embodiment, for ordering natural language texts (e.g., an "ebook"), software games, video and movies. Asynchronous transfer refers to the downloading of IP from one or more than one database using the wireless mobile device. The actual transfer of data takes place and is stored in a customer's SEC (security encryption compression) device. A user could utilize the IP at his or her discretion as opposed to real-time usage with a data stream transfer.

In one embodiment, multiple databases and portals with transparent links can be used and accessed with the mobile wireless device. It is immaterial to the practice of this embodiment of the present invention whether access is through mobile wireless or cable, fiber optics, telephone access to an Internet portal or database. The same end-to-end security as described in this invention for IP is consistent with the invention. The same dynamic encryption and mechanical and/or technical means exists throughout the data transfer distribution cycle. After the transfer occurs, the user (i.e., customer) SEC unit contains data and rules linked to data governed by the "smart" storage device. The smart storage device determines the time of autoerasure, watermarking, level of security from the highest strata to a more open system and other rules directly linked to that data or piece of the IP data. The rules can apply as minutely as a note, word or bit, etc.

Synchronous data transfer refers to a continuous stream of IP data to the mobile cellular device. Here, the same rules for the IP exist in real time and the wireless connection must be maintained throughout its transfer. A combination of synchronous and asynchronous transfer could exist within the database and multipurpose consumer device. A single purpose device, for example, one providing mobile wireless access to an internet music data portal without other functional abilities is also within the scope of the present invention.

In one embodiment, the wireless device can also be linked to other devices synchronously or asynchronously. For example, data transferred on the mobile wireless device after downloading a music IP could be transferred to a car or home stereo system, when music (audio) is played. Various transfer mechanisms can be used for the transfer of music or other IP. One embodiment of the present invention includes the transfer of IP through radio frequency to a car stereo or a home stereo, and the transfer of movies and television programs through radio frequency transfers to television sets and/or computers. In the case of a mobile wireless device such as a car stereo, the mobile wireless device is equipped with radio circuitry that can interface with the car stereo's AM or FM frequency. Transfers to this circuitry can be either synchronous or asynchronous. In a similar manner, the mobile wireless device could access other forms of IP, such as video, movies, software, text, and multimedia, etc., and transfer the IP in an encrypted manner, digitally secured as stipulated by a content owner's rules regarding the IP.

Digital content security can be produced and distributed in real time "on the fly." Professors, musicians, authors, instructors, film producers and any individual or organization or corporation can secure "their" content from redistribution when producing the content in a live setting or to be released on the web or other method of business-to-business or business-to-consumer digital distribution. The scope and quantity of content can be a word, note, picture frame based on DOI (Digital Object Identifier) or a complete or part of an entire work of art or content. Course packs present a classic example of bits and pieces of information gathering. The scope could also mean "on the fly content."

In one embodiment, rules formulated by content providers are matched with technological capabilities. The rules applied toward a certain content will constantly adjust in accordance to market demands, functionality and use of content as well as with technological advancement. The rules relative to a DOI, text, audio, visual, or content form will be tied to the content in a secured manner.

Digital content rules will be assigned with digital security to each and all content in any form (text, music, video, software, multimedia.) Such rules will be established by content owners and providers and will not be alterable or capable of manipulation by digital content users.

Functionality is defined as how content is allowed to be used. For example, the content (i.e., "text") can be autoerased, allowed to be printed or transferred to another user (or not), watermarked, and a host of rules applied governing activity, use, and manipulation of the content. The content can include natural language text, music, video, software, or multimedia. The rules regarding digital content and security also includes the tracking, accounting and verification of transactions.

Consolidation of intellectual property for content providers can exist in one master database or several databases or subsystems. Transparent links to outside databases to reserve intellectual property are used in one embodiment of the present invention to provide a customer with greater depth while giving content providers a sense of database control and management. Security, uniformity and integration are maintained throughout the system's network distribution chain. Customers may not know the location from which content is ultimately accessed. This seamless transfer greatly enhances content-driven access and continuity.

Since intellectual property content is fragmented into thousands of providers, content continuity and access is important to help mediate content sourcing and availability. A smart browsing and retrieval system that will, in effect, assist a consumer in accessing information by title, subject, author, artist, studio, publisher, etc., is built into the platform to be standardized. Embodiments of the present invention develop systems integration and an active digital distribution database that apply security access rules if needed, and then redistribute the information to business users, household users, and/or organizational users.

Customization, business users, household consumers, etc., can, if content providers allow via rules applied to the content, customize their content. This customization of content can extend to any form of digital intellectual property and polarity. In one embodiment, customers or content providers and integrators can add music to text material, animation, software, pictures, video, or multimedia. Cumulative printing or release play - music, video, etc. - is determined by content owners percentage of total content. A certain percentage of a song could be taken out of security, for example.

Advertising and promotions can be used to supplement supplier's income from IP and/or reduce the cost to customers. Content owners will decide, as will customers, to what extent advertisement will be embedded or linked to content, and thus, how much income will be supplemented and/or cost reduced.

Because of content security and use restrictions, digital content returns are made possible.

In one embodiment, autoerasure is provided based on a secured, unalterable (by a user or customer) calendar clock. The clock can be reset when the customer retrieves information via wireless, internet, or other means. Autoerasure rules include the elimination of title (i.e., file) access when time is expired. A customer could then reactivate the affected title access for an additional period of time. If a customer does not choose to renew a rental IP, the content of the IP is totally removed from the system.

B. System Architecture

Figure 1 illustrates one embodiment of the present information distribution system. The system is shown, for illustration purposes only, as being implemented across the world. Referring to Figures 1 and 2, one of the facilities provided is one or more "central data centers" or "central information banks" 100. Each central data center 100 acts in conjunction with any others present in the

network to store and control delivery of IP. Additional data centers 100 each comprising one or more computers acting in conjunction with each other are provided. A central information bank 100 is a central "library," or storage location, for information. Peripheral information banks 102A-F, coupled to central information bank 100, are libraries, or storage locations, for community oriented information. For example, the information stored in central information bank 100 accessed most often from the San Francisco bay area peripheral information bank 102A may not be accessed often from the peripheral information bank for Rome, Italy 102E. In any event, central information bank 100 is coupled to each peripheral information bank 102A-F to enable sharing of information. As explained in more detail hereinafter with respect to peripheral information bank 102F, each peripheral information bank 102A-F is coupled to one or more point-of-sale sites.

A central transactional database 104 coupled to the central information bank 100 and the peripheral information banks 102A-F, serves a central record keeping function for central information bank 100 and peripheral information banks 102A-F. Central information bank 100 and central transactional database 104 preferably, are commercially available main frame computers, such as an IBM main frame computer. The particular main frame model selected depends on the amount of information to be centrally stored in the network, the extent of record keeping functions to be performed, and the speed at which transfer and processing of information is to occur. Importantly, the present invention is not limited to any one particular computer to serve as the central information bank and/or the central transactional database.

As shown in Figure 1 is an exploded view of the various couplings between central information bank 100 and transactional database 104, peripheral information bank 102F and various point-of-sale delivery sites, particularly, point of purchase sites 108A-C, point of rental sites 110A-D, promotional sites 112A-D, and IP Bank subsystem sites 114A-C. Each point of purchase site 108 includes a point of purchase transactional database, represented by a box, and a user interface,

represented by a circle. As explained above, the user interface is sometimes referred to herein as the "IP Bank." Specifically, point of purchase site 108A contains IP Bank 116A and transactional database 118A, site 108B contains IP Bank 116B and transactional database 118B, and site 108C contains IP Bank 116C and transactional database 118C. Since the central information bank 100 and peripheral information bank 102F, and specifically peripheral information bank memory storage unit 106A, also could serve as IP Banks, such units are illustrated as circles. Further details regarding IP Banks and transactional databases are provided below in Section C.

As illustrated in Figure 1, each point-of-sale delivery system, such as systems 112A, 108A-B, 110A, and 114A-B, may be networked directly to peripheral information bank 102F, or the point-of-sale delivery system, such as systems 108C, 110B-D, 112B, 112D and 114B-C, may be networked to the point of purchase site 108B, which is networked to the peripheral information bank 102F. Point-of-sale delivery system configurations are explained in more detail below in Section C. At the level illustrated in Figure 1, however, it is important to understand that the delivery systems may be integrated into various combinations, such as a promotional point of rental system as shown by 110B and 112B, or a promotional point of purchase system as shown by 108B and 112C or a combination of a promotional, point of purchase, and point of rental systems as shown by 108C, 110D and 112D.

Communication network links between the central information bank 100 central transactional database 104, peripheral information banks 102A-F, and point of sale sites can be made utilizing one or a combination of many commercials available networks such as telephone, satellite or cable networks or any other medium suitable for transmitting information in digitized format. Many well-known protocols could be used in connection with the present system. For example, if the Internet is used as the "backbone" network, the well-known TCP/IP protocol could be used.

Figure 2 illustrates the flow of information in accordance with the embodiment of the system architecture illustrated in Figure 1. For ease of illustration

only, peripheral memory storage unit 106A is consolidated into central information bank 100, and peripheral transactional database 106B is consolidated into central transactional database 104. It should be understood, of course, that communication links between the peripheral information bank 102F and central information bank 100 and central transactional database 104 are provided.

As illustrated by the inputs provided to block 202, a publisher will receive inventory reports from the central information bank 100 and sales data from central transactional database 104. Based on this and other information the publisher can determine whether to place additional information on the netwerk. For ease of reference such information is sometimes referred to herein as "information titles" as shown in block 204. If the information is not present in an electronic format, then the information is digitized 206, disposed in an electronic format 208 and then undergoes electronic authoring 210. The digitized information is then transmitted to a data converter 212 for converting the digitized information into a uniform format. For example, if the central information bank 104 and central transactional database 104 are DOS- or UNIX-based systems, the data converter will convert the information into a DOS or UNIX format, as appropriate. If the information titles are in a digitized format, the information titles are transmitted directly to data converter 212 for direct conversion into the uniform format as illustrated by line 214.

Once the data is in a uniform, digitized format, it undergoes an initial encryption and compression to both reduce the amount of storage space required to store the data and to make the data ready for being transmitted with less risk of unauthorized use while being transmitted through a communications network. The compression is accomplished through the use of one of the commercially available compression protocols. The initial encryption is performed using one of the standard available encryption protocols as discussed below in Section D.

Once in uniform, encrypted and digitized form, the information titles are stored in central information bank 100. An electronic index listing all titles

available and accessible by author, title, subject or ISBN codes and/or ISSN codes is prepared. As new information titles are added, the electronic index is updated to include the new titles. The information titles may then be downloaded to IP Bank 116A. The information titles and corresponding electronic index information may, in addition to or rather than being stored in central information bank 100, be disposed on laser disk masters as illustrated at block 216. Laser disk masters 216 can then be installed directly into IP Bank 116A.

In one embodiment, as desired information data titles are being downloaded from IP Bank 116A to a user's storage medium 218, each file is being dynamically encrypted and encoded with authorization and user identification data to restrict access and user of the information being transferred. The encryption process uses algorithms and formulae generated using a combination of the unique serial number of the storage medium to which the encrypted file is to be downloaded, the unique registration number given the user requesting the downloading at the time of registration and the unique hidden number given the file, a copy of which is to be downloaded. In this manner, the data being downloaded is tied to the user requesting the downloading and the storage medium on which the encrypted data is to be stored. The unique serial number of the storage medium may be a number that is permanently associated with and stored upon the storage medium at the time of manufacture or initial formatting or may be a number that is electronically generated and assigned when the storage medium is initially registered with the system. In both cases the number will be electronically readable and stored on a nonvolatile portion of the memory storage space associated with the user storage medium. In one embodiment, a current time and date are included with the data titles downloaded from IP Bank 116A so that a check is made of a clock associated with user storage medium 218 or an associated user device to ensure that no backdating of the clock in end user's device has taken place.

Prior to downloading desired information titles, the user may access an electronic index which contains all the information titles available for downloading

from IP Bank 116A. Through the electronic index, the user obtains the listing for available information titles by author's name, by specific title of the work, by ISBN code or by subject matter. Once compiled, a listing of the available information titles included in the index category selected and the other necessary information to allow the user to purchase or rent any information title contained in the index category listed is displayed on the video screen. Using the video listing, the user selects any title listed thereon and obtains a printout of the relevant information through the printer slot 342. Upon proper access by a user, the information titles may then be downloaded from IP Bank 116A onto a user's storage medium 218.

After downloading of information and corresponding electronic index information form central information bank 100 or installation of laser masters 216 to IP Bank 116A, inventory reports are generated by IP Bank 116A and transmitted to central information bank 100. These inventory reports reflect the information titles presently stored in IP Bank 116A. These reports are then are sent to publisher 202. Also, a download completion report is sent from IP Bank 116A to transactional database 118A, sometimes referred to herein as a host fileserver, which in turn generates a status sales report. The sales report is transmitted to central transactional database 104. Transactional database 104 sends the necessary action instruction back to host fileserver 118A and a transaction report to publisher 202 for uses such as accounting and auditing.

The cartridge also contains programming (CCS) that regulates access and use of encrypted data files, decrypted an encrypted file when selected for opening, controls the operation of the user's computer when a decrypted version of an encrypted file is being accessed, and removes all trace of any decrypted version of an encrypted file from the user's hard drive or RAM when being closed. (RAM may include or consist of DRAM, SDRAM, and/or VRAM).

In one embodiment, a content provider can specify instructions relating to authorized use, access and cost of the provided information that can be permanently

linked to a master data file of the information when it is electronically stored or accessed. Instructions are electronically generated when information is received electronically. These instructions include a description of allowed uses (e.g., copy generation, printing limits and/or authorization, rental options, if any, purchase options, etc.), desired level of security against unauthorized copying or use (from level zero [virtually no security] to a maximum level [most robust security available]) and cost to a user, optionally as a function of user-selected access right. Whenever a request is made to obtain a copy of the information file (i.e., IP File), the instructions are used in connection with the choices made by the user, within the allowed options, to generate user-specific electronic instructions for limiting use of the requested copy of the IP File. For example, content providers who wish to allow a user to be able to produce a hard printed copy of a portion of an information file for study purposes, when the information files are being downloaded into the master file, can select that special authorization codes be included with the master data file. Once established, the instruction codes so generated accompany the information file to the storage medium, or cartridge, of the user and regulate the use of the information file by the user. The cartridge retains information relating to such printing and restricts further printing once the limits have been reached. The user determines, within the defined limits, or authorized purposes, the portion of the text (natural language text or other IP) to be produced as a hard copy by using the high lighting features of the reader programming to make a selection. In one embodiment, if no special codes are selected, default codes apply that embody the most restrictive instruction selections. In another embodiment, the content provider can allow the user to select the applicable use and access instructions from a variety of authorized choices with the selection being made at the time of acquisition. The cost of acquisition to be paid by a user will vary based upon the user choices regarding desired use. In one embodiment, rules can be updated or adjusted by a content provider.

In another embodiment of the present invention, when one or more IP Banks are operated in conjunction with one or more retail establishments, each retail establishment is given a unique identification number that is used to tag each user

device, user storage medium and/or encrypted IP file acquired at the retail establishment or through an IP Bank linked to the retail establishment. Using the tagged information, particular user devices, storage media and/or IP files, a predetermined portion of the system revenue generated in regard to such tagged user devices, storage media and/or IP files is allocated to and shared with the retail establishment in question. In another embodiment, the tagging is further delineated to allow revenue sharing with manufacturers and distributors of user devices and/or storage media.

C. Point-of-Sale Delivery System Configurations

The point-of-sale delivery systems, as previously discussed, are classified by function. The functions include one or more of the following: (1) point of purchase delivery system, (2) point of rental delivery system, (3) IP bank subsystem, and (4) promotional delivery system. The configurations for each of these functions are separately discussed in detail below.

Point of Purchase Delivery System

A point of purchase system is illustrated in block form in Figure 3. The point of purchase system is described herein for illustration purposes only as a system from which IP can be purchased. As pointed out above, however, the system is not limited to a particular type of IP and other media capable of being expressed in electronic form such as computer software, music and video could be purchased utilizing the present system. In addition, although the system described here is a point-of-purchase delivery system, other embodiments employ either synchronous or asynchronous IP network protection, or both, making possible real-time IP transmission.

The point of purchase system illustrated in Figure 3 includes an IP Bank 302 coupled to host fileserver 304. Server 304 is coupled to a customer service terminal 306 (of course, there could be more than one terminal) and a cashier's station

308A which is further interconnected to other cashier stations 308B-D. Server 304 also is coupled to an institution network 310, which in turn connects to institution terminals 312A-E. Service terminal 306, cashier stations 304A-D and institution network 310 are connected to server 304 via a computer communication link such as a commercially available computer networking system such as CompuServe, a public network such as the Internet, an intranet, or a virtual private network (VPN). IP Bank 302 and server 304 are connected to central information bank 100 and central transactional database 104 as explained above with reference to Figs. 1 and 2.

Cashier stations 308A-D are in serial, linear networking connections which allows the addition and removal of a number of cashier stations at any time. This configuration accommodates extra cashier stations required during rush seasons or rush hours and the desire to remove cashier stations for better utilization of space after the rush seasons. Customer service terminal 306 has local processing capability that provides customer services such as personal identification initiation, personal identification number changes, processing of complimentary IP, IP refunds, customer information entries and updates. The customer services terminal 306 can also provide the retail outlet with internal administration and the management functions, such as the IP inventory cards management, the IP list management, IP requests, IP reports, financial reports, and e-mail and Bulletin Board management.

Referring now to Figure 4, point of purchase fileserver 304 is shown in more detail. Particularly, server 304 includes one or more central processing units (CPUs) 316, a primary power supply 318, an uninterrupted power supply 320 to assure continuous operation during power failure, and a high density storage 322 that holds all the programs and the databases required for server 304 operation.

Server 304 has four (4) interfaces, i.e., a network interface 324, a maintenance interface 326, a customer service station interface 328 and a cashier station interface 330. CPU 316 transmits instructions to IP Bank 302, creates

transaction databases and reports, and processes orders from cashier stations 308A-D and customer service terminals 306A-D.

From network interface 324, server 304 communicates with central transaction database 104 for electronic filing of transaction reports and communicates with IP Bank 302 to give IP Bank 302 downloading instruction orders and to receive the status reports and the inventory reports from IP Bank 302. Server 304 also is coupled, through network interface 324 to an IP Bank subsystem to receive subsystem reports in order to give instructions and orders whenever necessary, as hereinafter discussed. External network systems such as institutional or corporate network systems with local merchants terminals, community bulletin board services and others can also be coupled to the network interface 324. The network interface 324 also allows two-way connecting with inter-bank networks such as Cirrus, Plus or other similar data transfer network. Coupling to merchants' terminals, promotional system provides local merchants and the local business direct access to update their promotions and coupons. Maintenance interface 326 enables remote or on-site diagnosis and repair of server 304.

Customer service station interface 328 provides for communication between server 304 and customer service terminals 306A-D to handle customer service transactions. Customer service terminals 306A-D are illustrated as being coupled through a data switch 332 to a printer 334. Cashier station interface 330 provides that cashier stations 308A-D can communicate with server 304.

Figure 5 illustrates one embodiment of IP Bank 302. IP Bank 302 includes a high resolution color graphic display 336 which is a touch screen device used to display, for example, instructions, messages, and status reports to the user, indexing information and to receive the user's touch screen input selections. IP Bank 302 also has a keypad 338 that is for the user to input a personal identification as well as other inputs. A magnetic code or other generally accepted card reader 341, shown as an insertion slot, is provided for customers' transactions with a bank card, credit

card or some other form of debit card. A bar code reader 340, shown as an insertion slot, is provided to allow users to insert cards containing ISBN and/or ISSN codes for desired information titles for reading by the IP Bank. ISBN and/or ISSN codes may also be manually inserted, for example, by typing the relevant numbered keys on the keypad 338 or with a joystick type device (not shown). A printer slot 342 also is provided to enable the user to access the output of IP Bank 302, a printer (not shown in Fig. 5), as hereinafter described, to retrieve receipts and transactions reports and ISBN access vouchers. IP Bank 302 also includes a base member 344 with a cut-out portion 346 to enable a user to stand comfortably at keypad 338. Other configurations are possible for users having special physical needs. Importantly, IP Bank 302 also includes a cartridge slot 348 for the user to input a reading cartridge, as explained in detail hereinafter, to obtain a copy of the information selected for downloading.

In another embodiment and as shown in Figure 5A, the physical embodiment of IP Bank 302 may be altered. More specifically and in one embodiment, IP Bank 302 is positioned on a desk 339 using a personal computer 349, for example those available from IBM Corporation or Dell. The user operates IP Bank 302 as described above with reference to Figure 5 except, the user may for example, sit in a chair (not shown). Such a configuration may be used, for example, in a corporate, dormitory, library, or other similar environment where the user may be accessing information for longer periods of time or in a professional type environment. In other embodiments, readers 340 and 341and cartridge slot 348 each may be located within computer 349 or in separate devices which are electrically coupled to computer 349.

In yet another embodiment of the invention, and as is shown in Figure 5B, a different physical embodiment of the IP Bank 302 is provided. More specifically, IP Bank 302 is placed in proximity to central information data storage facility 100 and is in electronic communication with central information data storage facility 100 via any suitable means (e.g., cable, wireless, etc.). In this embodiment, IP Bank 302 is contained within a housing 500 for combined central storage 100 and IP

Bank 302. User access to IP Bank 302 is via dial-up modem 502, 512 over the telephone, via the Internet through a web site 504, 506 maintained for that purpose, via satellite linking, via wireless (such as narrowband wireless, broadband wireless, infrared, microwave, radio wave or other similar connection) or via any other network capable of electronically transmitting data in digital form, for example, a cable modem, ADSL-X or broadband wireless network. Once IP Bank 302 is accessed by the user using specialized software contain in a WORM (write once, read many times) memory or other nonvolatile memory on the IP Bank and on the user's storage medium 218, a virtual IP Bank is generated for viewing and access using the user's computer. The virtual IP Bank then performs all of the same functions as IP Bank 302 in another embodiment, except that memory of central information storage facility 100 is used as storage for the information titles and the transaction information, the appropriate hardware connected to the user's computer operates as an access port to IP Bank 302, and specialized software programming stored on the user's storage medium in connection with specialized software programming stored on the WORM (write once, read many times) memory of the IP Bank operates as the software programming to drive the IP Bank.

In yet another embodiment of the invention, IP Bank 302 is a special board configuration located within the user's computer or a separate device electronically linked to the user's computer by a cable, a phone line, a wireless connection (infrared, microwave or otherwise) or any other suitable means. In this embodiment, IP Bank 302 is configured in such a manner that any attempt to read the data contained thereon other than as authorized renders the data totally unreadable. IP Bank 302, in this embodiment, is connected to the central information storage facility 100 or another IP Bank 302 using a secure network. In one embodiment, IP Bank 302 also functions as a controller of the user's computer when being used to access encrypted files or the secure network. In this embodiment, IP Bank 302 also contains operating software that is stored in WORM (write once, read many times) memory within IP Bank 302.

Figure 6 is a block diagram description of IP Bank 302 circuitry. Particularly, IP Bank 302 includes a central processing unit (CPU) 350, which is coupled to display 336, keypad 338, magnetic strip reader 341 and bar code reader 340. Although CPU 350 is illustrated as one unit, it is contemplated that CPU 350 could be a parallel processor or distributed processor arrangement. Selection of CPU 350 type depends on the amount of information to be processed, the desired speed of processing and costs. CPU 350 also is coupled to an automatic teller machine (ATM) module 352 to allow transactions with ATM cards. CPU 350 is coupled to a media driver 354 which enables users to insert personalized media for acknowledgment or other functions as hereinafter discussed. IP Bank 302 also includes a primary local storage device 356 provided for the storage of all information masters selected for loading into IP Bank 302 and related index information. A secondary storage device 358 is provided to hold other programs, instructions and transaction related information. A buffer memory 360 is utilized to speed up downloading in order to accommodate high volume users during the peak seasons. A printer 362 is provided to print coupons on demand, receipts and various reports for the users. A power supply 364 provides power to printer 362. CPU 350, secondary storage device 358 and local storage 356. An uninterrupted power supply 366 coupled to primary power supply 364 assures continuous operation even during power down time.

CPU 350 is coupled to a network interface 368 to provide communication to central information bank 100, host fileserver 304 or an IP Bank subsystem, as hereinafter discussed. CPU 350 also is coupled to a wireless communication port 370, which in turn is coupled to an antenna 372. Wireless communication port 370 enables compatibility with an alternative communication medium in the event that such medium is required.

Figure 7 illustrates, in block diagram form, the structure for a user's personalized media storage cartridge 374. As explained hereinafter, a user inserts cartridge 374 into cartridge slot 348 for downloading of the information selected from IP Bank 302. The downloaded information is stored, in an encrypted format, on

cartridge 374 together with relevant basic index information copied from the electronic index contained in IP Bank 202 at the time of initial downloading. Cartridge 374 is compatible with readers to enable the user to view information stored on the cartridge. Cartridge 374 includes reading software 376 that, as explained in more detail hereinafter, performs sequential encryption and decryption of information. Registry correspondence segment 378 also is provided. an IP file registry 380 is created at the time of downloading information onto cartridge 374. Encrypted IP files 382 together with relevant electronic index information are stored on cartridge 374 as well as a non-erasable permanently marked serial number 384. Cartridge 374 also contains a commercial operating system environment 386 and free disk space 388.

In another embodiment of IP Bank 304, slot 348 is a part of a device connected to the user's computer being used to access the encrypted files.

Figure 8 illustrates the user process and component processing which occurs when a user utilizes the point-of-purchase system described above. Particularly, once the user enters the site 390, and if the user a first-time patron 392, the user will complete a user's application form 394. The user will then take the completed application and a picture I.D. to customer service station 306A, where the user will select and input a personal identification number (PIN) and a password 396. The customer service clerk will open an account for the customer 398. The user-selected password is automatically matched with a sequentially created customer account number within the central data banks. Using the keypad accompanying the cashier station, the clerk types in the name, address and social security number for the user. The written application will then be inserted into the printer slot accompanying the cashier station. While loading the customers' information, the central data bank reviews the information to determine if there are any prior problems with the customer or other discrepancies. When the verification process is completed, the designated customer account number for the user is printed on the user's application. Then, the clerk places, into the card slot, a user identification card (for example, a plastic card having dimensions of the standard credit card and containing a magnetic

strip on the back on which can be placed magnetic coded information). The card is then embossed with the user's name and account number and the magnetic strip is encoded with the applicable user codes (account number, card number and designated password information). The written application is then transmitted to the central data storage center for retention. The user now is able to use the issued card to make purchases or to rent the use of information titles. The machine used to emboss and encode the cards is a standard commercially available machine of the type currently being used in connection with the issuance of a bank's card, credit cards or debit cards. Using the password supplied by the user and the application registration number, a unique user identification number is electronically generated. This identification number is then magnetically stored on the magnetic strip on the back of the user's card and within the data files of the machine generating the embossed card. This information is stored in an encrypted file later transmitted to central information storage facility 100 using a suitable secure network. The unique number so generated is used to represent a personal signature (system registration number) of the user with regard to access to the system and encrypted files.

A user may also obtain a personal identification card by accessing the system, through a network, and by supplying the necessary information for the generation of a user identification file. Upon completion of the registration process, the user electronically receives a digital identification file and identification number (or password). At the time of registration, the user is assigned a unique account number that is associated with his or her data files within the system for accounting and tracking purposes. A digital file containing the assigned account number, the user identification number and the applicable selected password information represents the identification file. After the identification file has been stored, the user may obtain a printed copy of the relevant information contained in said file. At the same time as the identification file is being generated, the system programming generates a unique number using a combination of the user account number and the numeric equivalent of the user password. An electronic version of that unique number represents the electronic personal signature (registration number) for the user. A digital copy of the

unique number is stored with the user's identification file using a special encryption method. Only the public (non-hidden) portion of the data is available for printing to hard copy. The digital identification file is available to be used in tagging and encrypting data files and allowing access to the network and encrypted data files. A copy of the registration file, including a copy of the identification file, is stored at central information storage facility 100.

In addition to obtaining a personal identification card, a new enrollee purchases a reader/computer or other acceptable reading device (such as a special computerized interface, or an audio or video playback device). Each such device is assigned a unique serial number and a special code number. In one embodiment, the serial number is contained on a read only memory chip enclosed within the device. All of the many cartridges which accompany each such reading device is encoded in such a manner that information recorded on the cartridge can only be read by the related reading device. In one embodiment of the invention, this is accomplished by a simple program contained within the permanent memory of the device. In another embodiment, if the special code on the device is not the same as the number which the cartridge is seeking, then the cartridge will cause to be displayed in the reading device the words "cartridge cannot be read by this device" and to not allow any further access to any information contained on the cartridge by the particular reading device in question. If the numbers match, further access will be allowed. At the time a reading device is purchased, the clerk enters the serial number for the device into the central data bank through the cashier's station. The central data bank contains a list of the serial numbers of all approved reading devices and the corresponding special code number. The personal identification card for the customer purchasing the reading device is placed by the clerk into an appropriate slot on the cashier's station and the magnetic strip on the identification card is encoded with the applicable serial number for the reading device being purchased. Thereafter, whenever the user desires to obtain additional cartridges for reading by his or her reading device, the user needs only present his personal identification card and the cartridge to be properly coded to the clerk and by inserting the cartridge into the cartridge slot and the identification

card into the card slot and pressing the designated button on the cashiers station, the new cartridge will be correctly encoded to be readable by the user's reading device.

In another embodiment of the invention, the personal identification number given a user at the time of registration, the unique serial number of the user's storage medium being used to store the downloaded files and a hidden unique number given the content being copied for downloading are used to generate unique encryption and decryption algorithms and formulae. A copy of the algorithms and formulae so generated are stored in the central information storage facility. The encryption formula so generated is used to encrypt the data files as they are being downloaded and stored on the user's storage medium. The decryption formula and algorithms are stored in nonvolatile memory associated with the user's storage medium and are available for decryption when access to an encrypted file is requested. The memory unit and the housing thereof, where the decryption formula and algorithms are stored when downloaded to the user's storage medium, are configured so that any attempt to read the information so stored, other than through the use of the CCS software and related operating programming, renders the data unreadable in any manner. WORM memory is used in one embodiment of the memory unit.

The requirement that reading device codes and cartridge codes match, before access will be allowed, means that issued cartridges will not be readily readable by multiple reading devices. Multiple device reading will require special programming and the granting of special allowances, or approved purposes. In one embodiment, by purpose encoding the information, a publisher may expand or limit access to those users having a proper authorization or defined purpose. For example, a publisher may purpose encode a portion of a selected IP to be readable by any user, i.e., any purpose encoded. This type of purpose encoding may be used on, for example, promotional IP or some governmental publications. Other information may be purpose encoded to limit access to a single user to only view the information, i.e., classified material. The requirement reduces the possibility of unauthorized use of

information titles. Special allowances also can include various security code levels that allow publisher studios and content owners the ability to choose between a wide variety of security from completely open to the highest level in which the content of an IP can only be utilized by one individual. Security codes and special allowance rules for content owners could, for example, be determined by the market value of the content. The life cycle of the content can also be considered, so that new edition music, movie release, and new computer games have different security compared to content that has been in the market for an extended period of time. In staging security related to time value, market value, control level, type of intellectual property, or even legality, the highest level of security, in one embodiment, is the use of the highest security encryption algorithm with a hardware smart chip or smart storage device controller chip or processor.

In another embodiment in which IP Bank 302 is located either in proximity to central information storage facility 100 or in proximity to the user's computer, the user's storage medium is encoded with the applicable registration codes and numbers by use of the appropriate slot on either the user's computer or IP Bank 302, were a separate external unit is being used as such. With the appropriate software activated, the user inserts the applicable storage medium into the appropriate slot and using the appropriate software menu selects the appropriate instruction. The software programming then develops the appropriate registration information and encodes it on the storage medium in the appropriate manner. As part of the initiating process, the software programming checks the storage medium to make sure that it already contains the appropriate CCS. A user storage medium that does not already have a unique serial or identification number is given one and, and any user storage medium that does not accept electronically being tagged with a serial number in a appropriate manner is rejected and so marked. Only user storage media containing the proper software programs and registration information are usable to store data information files.

In operation, the customer takes the customer identification card to the IP display area for shopping 400. If the customer previously opened an account, the customer will not have to go through the above described process and can proceed directly to shopping area 400, where the customer will select an IP inventory card matching his IP selection. The IP inventory card has the IP ISBN and/or ISSN numbers, a bar code and information related to the particular information title, author, publisher, and edition date printed thereon. The customer brings the selected IP inventory card to the cashier's station 308A. The cashier magnetically reads the codes on the customer's I.D. card and scans or manually enters the bar codes on IP inventory cards 402. The customer then makes a proper payment, and the customer codes and information title bar codes are transmitted to host fileserver 304. Server 304 searches the existing customer account file to match the identification (i.e., pin and password) and will generate a downloaded IP list file based on the bar codes from the IP inventory cards or as manually loaded. Server 304 downloads the file to IP Bank 302 which electronically generates a portfolio of information titles ready to be downloaded on demand. The user can then proceed to IP Bank 302 at any later time and insert the identification card into the slot 340 of IP Bank 302 and a coded point-of-purchase cartridge 374 into IP Bank cartridge slot 348 to identify himself with a personal identification number, as illustrated in step 404. The user also enters a password 406 into the keypad 338. When IP Bank CPU 350 matches the personal identification number with a downloaded list portfolio, IP Bank CPU 350 starts downloading the requested information from local storage 356, through buffer memory 360, to media driver 354 which copies the information onto cartridge 374. As part of the downloading process, the data is dynamically encrypted to make the data uniquely readable only by authorized reading devices. The dynamic encrypting is described below in Section D. After downloading, the user removes cartridge 374 and then inserts cartridge 374 into his personal reader/computer to access the information acquired. The reader/computers are configured for long-term reading applications. The reading application software is stored on cartridges with the ability

to read the applicable software on the cartridges permanently stored within the memory of the reader/computers or other authorized reading device.

A user may select portions of selected information to combine and download. In one embodiment, the user may select at least one IP and select at least one portion of each selected IP. If more than one portion is selected, where each portion includes up to the entire selected IP, the portions are combined and downloaded to user's cartridge 374. For example, for a specific college course, a student may be required to download specific chapters from ten different IP. After selecting the ten IP and ten specific chapters of the selected IP, the selected information is combined, encrypted using the determined level of protection, and downloaded to the students cartridge 374. Similarly, a user may select individual tracks from music information to combine and download the selected tracks to a single cartridge 374 for playback at a later time.

In another embodiment in which IP Bank 302 comprises hardware and software in the user's computer and hardware and software located other than in proximity to the user's computer (e.g., an IP Bank located proximate to central information storage facility 100 or a stand alone IP Bank located apart from the user's computer and central information storage facility 100), after connecting to the IP Bank unit 100, using the appropriate browser software, the user will access the central storage facility 100 index of available titles and select the desired titles or parts of titles that the user wishes to purchase. From this information (from which a work is created that represents a portion of several different works), IP Bank 302 will cause to be generated a unique identification number for the newly created work. This unique identification number is generated in addition to any hidden code that is generated and serves as an index reference for the work. IP Bank 302 also uses the user's request to generate a shopping list with appropriate price information, which the user may accept as generated or change. When the list is accepted by the user, the menu requests payment information. Generally, at the IP Bank level, payment is via pre-generated credit voucher or via credit or debit cards. After payment approval, IP

Bank 302 causes copies of the requested titles to be generated, encrypted, and downloaded on to the user's storage medium. While connected to the user's computer and storage medium, IP Bank 302 examines the appropriate log files to determine whether there has been any misuse or unauthorized activities. If such a determination is made, the account is flagged for further investigation.

Point of Rental Delivery System

If a user is not interested in obtaining a permanent copy of a particular work but requires a copy for a period of time, e.g., a semester, the user may prefer to visit a point of rental site rather than a point of purchase site. A point of rental system is illustrated in Figure 9. The rental system is identical to the point of purchase system previously described herein (e.g., includes a host fileserver) except with respect to the differences pointed out below. In many instances, a single site or IP Bank may serve as a point of purchase system site and a point of rental system site and a point of delivery system for promotional or commercial information site or any combination thereof. As shown in Figure 9, the point of rental system includes IP Bank user terminal hubs 410A-B coupled to terminals 412A-E, and customer service station 414. User terminals 412A-E allow a customer to do an information title search and index search of the IP Bank memory and to transmit other information between IP Bank 302 and himself. Customer service station 414 combines the function of customer service as well as the cashier's station. For example, at customer service station 414, a credit customers' debit card can be credited and the ATM operation can be overridden, via ATM module 416, if necessary. Information can be printed out from customer service station 414 via printer 418.

Point of rental storage medium 420 is used in the rental system. Point of rental medium 420 is the same as point of purchase medium 374 except that medium 420 includes an automatic erasure mechanism that erases the information downloaded after the expiration of a preset time interval. More specifically, when information is downloaded from IP Bank 302 onto medium 420, IP Bank 302 also

downloads a "time stamp" (using a nonvolatile, time-encoded chip that cannot be manipulated) equal to the time period for which the user has paid to retain a copy of the information. The time stamp could take the form of a value loaded into a memory location on medium 420, which value corresponds to the rental time period. During usage, the actual usage time elapsed is subtracted from the electronically stamped time period. Once the user has consumed all of the usage hours or other time units authorized, the information title will self-destruct, i.e., be deleted from medium 420. This can be achieved simply by calling a stored program which erases the information associated with the memory location where the time value is stored. For example, when the value of the memory location where the authorized usage time is stored is zero, the stored erase program would be called upon to erase the information associated with the "zero" time usage authorization. In one embodiment, an advance alert feature is provided to allow the user time to pay for additional authorized use before the information is erased.

Another method for automatic erasure is for each rental or library cartridge to contain a real time clock and independent rechargeable power supply. When the cartridge is initially encoded for use, the real time clock mechanism is activated. As rented information titles are being downloaded, an expiration date is logged into the index information for each title. Any time after the real time clock on the cartridge reaches the designated expiration date, access to the relevant information title is denied. If use of the title is not extended, after the expiration of an additional number of days, use of the cartridge will cause a permanent erasure of the information title from the cartridge memory. With this method, if the real time clock falls to operate, the cartridge will become unreadable without repair. To repair a defective cartridge, the user need only bring the cartridge together with his personal identification card to the nearest service center where the real time clock will either be repaired or the relevant information titles will be loaded onto a replacement cartridge. The user will be credited for any lost time while the cartridge was unreadable. A service center could be located, for example, near each separate point of delivery site.

In one embodiment, GMT clock verification is added to the user device, to provide additional IP security in case the user travels with his device through time zones. An encrypted GMT code is added in another embodiment to compare and verify erasure dates and times with actual GMT.

The automatic erasure program could be created as an operating system module or as a separate executable program designed to be "terminate and stay resident" (TSR). A module integral with the operating system is preferred since such a structure ensures that if the operating system is viable, the automatic erasure module is viable.

If the user still needs more time with any particular information titles, the user may return to the point of rental site and "re-rent" the information. Alternatively, it is contemplated that the user could renew the rental via a modem coupled to the reader.

With respect to the user process for renting information, when a point of rental patron enters a point of rental site, the user will use a valid ATM card, bank card, credit card, or some other debit card and proceed directly to a user terminal 412A-E. Using such a terminal, the user can perform information title searching and download an order entry to IP Bank 302. When the download entry is complete, the user will go to IP Bank 302, insert a rental medium, an identification card, and a credit card, bank card, or debit card into IP Bank 302 for the transaction approval. If the transaction is not cleared or if the ATM system is not working properly, the patron can proceed to the customer service center and have the attendant manually override the ATM process, if appropriate. If the user does not have a valid ATM credit card or debit card, the user will go to the customer service center, pay the service clerk to receive credit on the IP Bank debit card. Then the customer may proceed to the user terminal where the user downloads the order entry.

After the transaction approval is cleared, the patron inserts point of rental medium 420 into IP Bank media driver 354, has his personal identification card

scanned and enters a password. The information is dynamically encrypted and downloaded from IP Bank 302 to medium 420 with an electronic stamp of the number of hours of usage authorized for each information title or an expiration date. After the downloading, the user will apply this medium on the personal reader/computer to access the information on the medium.

Typical examples for the point of rental site are libraries (commercial, education or public access) and IP rental shops. The information downloaded by the user may be free of charge to the users such as in the case of a library, or may incur certain rental fees at a predetermined rate, such as in the case of a rental shop or library charging on a per page use basis. Any given point of rental site may operate as a traditional library in allowing free use to library members for a limited period of time or may operate as a rental shop where fees are collected from users in accordance with the period of use allowed.

IP Bank Subsystem

A IP Bank subsystem couples to an IP Bank and host fileserver as described in more detail below. The central element of the subsystem is an IP Bank which is a modified version of the point-of-purchase IP Bank 302. The subsystem is specifically configured for the collective use by members or the staff of a commercial or business entity or a corporation. It delivers and it recalls information titles among authorized users within the business or corporate entity, and provides the capability of limiting the number of copies of a given work that may be distributed to other authorized users. If all of the licensed copies of any information titles have been checked out by the staff of an organization, then no other users may access the same information title within that particular subsystem until one or more of the licensed copies of the particular information is uploaded or recalled to the subsystem or additional copies are purchased. In one embodiment, the information is purpose encoded so as to limit a purpose to which access by a user to the information is allowed. For example, a central corporate library may allow specific users, i.e., R&D

personnel, to selected information, i.e., pending patent applications. All non-R&D personnel users without the proper purpose, or authorization code, are prevented from accessing the information.

Instead of purchasing the unlimited use of a limited number of copies, a commercial or business entity may lease the limited use of an unlimited number of copies or the use of a specified portion of a given information title. Under such circumstances, the commercial or business entity would be charged each time the subsystem is accessed from a participating work station for the portion of a specified information titled accessed and for the period of time the access occurs. By restrictions encoded on the interface between a participating work station and the subsystem, while accessing information from the subsystem, the ability of the work station to perform certain operations would be restricted. The restricted operations would be those related to the duplication or transmission of data related to information titles being accessed through the subsystem.

More specifically, and referring to Figure 10, IP Bank subsystem 422 contains a high resolution color graphic display 424 coupled to CPU 426 to display the instructions or status of subsystem 422. Subsystem 422 also includes a keyboard 428 with limited access to the system for keying selections for operating certain given functions such as product display. (In one embodiment, a voice recognition system is used for input in place of keyboard 428 or to provide additional input capability.) Subsystem 422 has a media driver 430 for the downloading of information and a local storage 432 which holds a portfolio of information the business entity has ordered for use. A secondary storage 434 is also provided to hold all the software programs that control and perform the functions of subsystem 422. Subsystem 422 further includes a power supply 436 and an uninterrupted power supply 438 to assure continuous operation during power failure downtime. A printer 440 is provided to print various reports.

IP Bank subsystem 422 has a network interface 442 that connects subsystem 422 to IP Bank 302 and host fileserver 304. Network interface 442 also may couple to the corporate or business entity network system 444. With such a structure, the corporate entity may transmit or download its own corporate proprietary information through IP Bank subsystem 422.

Media port extension interface 446 provides access by an adequate number of media drivers to the desired corporate terminals for corporate network stations. Media driver 430 is connected to the terminals or stations by a proprietor driver card. The corporate administration can utilize the dynamic encryption and the dynamic downloading function of IP Bank subsystem 422 to incorporate and accommodate the corporate proprietary information. The corporate proprietary information may be transmitted to IP Bank subsystem 422 using an encryption process and then downloaded selectively to the destination port and to the properly identified authorized personnel. IP Bank subsystem 422 is not only a customized corporate library of copyrighted and proprietary information, but also is a corporate document security device that encrypts and dispatches the corporate documents and the corporate confidential proprietary information in the corporate network system. As part of the network interface connection linking each participating work station to the subsystem and allowing access to encrypted information, a separate unit, e.g., a memory storage unit restricts certain operations which may be performed from the work station so long as the work station has access to encrypted information from the subsystem. The restrictions limit or prevent operations related to the duplication or transmission of data.

Promotional Delivery System

The promotional system is a point of delivery system for promotional and commercial information. It distributes promotional and commercial information in electronic format and users may either view the digitized promotional and commercial information at the site or download the information to their personalized

media for later viewing. User's call access the promotional and commercial information including the dynamic viewing electronically of advertising available discounts, commercials, special promotional events, software demos and product catalogs. Users may even shop electronically by manipulating the promotional and commercial information and placing orders through e-mail from a personal reader/computer or by ordering directly from an interactive promotional IP Bank. The promotional IP Bank has the same structure as IP Bank 302 for the point-of-purchase system.

A promotional system in accordance with the present invention is illustrated in block diagram form in Figure 11. As in the other point-of-sale systems, IP Bank 302 is networked to host fileserver 304. The promotional system further includes a number of promotional units 448A-D which electronically display and promote products. Unit 448A is coupled directly to central transactional database 104 and central information bank 100 while units 448B-D are coupled to host fileserver 304. Unit 448A receives information from merchant terminals 450-A-D and host fileserver 304, receives information via merchant terminals 450E-G. More specifically, host fileserver 304 receives advertising and special offer updates from the local businesses, national or regional advertisers, and corporate sponsors through merchants terminals (MT) 450E-G. The host fileserver 304 is also networked to a central transaction database which, in turn, provides a report to the publishers, advertisers, accounting, auditing firms, merchandise vendors, and others.

The promotional IP Bank allows selective downloading of promotional and commercial information to the user's point of rental medium (see discussion in Section B, System Architecture, for explanation of such downloading) for the user's private review and personal shopping at his convenience. The promotional and the commercial information downloaded will self-destruct (i.e., automatically erase) at the expiration of a pre-determined time interval as explained above with respect to point of rental delivery systems. The promotional IP Bank also provides a user interactive self-service vending feature. The user may order products or information

electronically via the network. Some of the promotional functions are: coupons on demand, virtual shopping, catalog sales, demos, subscription orders, electronic applications of credit cards, calling cards, or other types of services. Some public domain information distributed such as community events, ticket sales, institutional events or even public bulletins could also be distributed with the promotional information as a free or low cost service to the community.

The promotional and the commercial information flow is very similar to the information flow within the point-of-sale delivery system. However, rather than a publisher or copyright information owners, the information sources are local businesses, national or regional advertisers, and appropriate sponsors through advertising agents and other entities.

Information Tracking

In one embodiment, for each exchange, or download, of information, a tracking entry is transmitted, or stored, in an appropriate transactional database, for example central transactional database 104, to record movement, or transfer, of information from a first location to a second location. By reviewing these tracking entries, an information owner may monitor movement of the information and take appropriate action. For example, a tracking entry may be recorded in transactional database 104 each time any information is copied into, removed from, or copied from, IP Bank 302. Based upon the tracking entries, the information owner may charge the receiving or transferring party a fee as defined by the owner of the information. The fee charged may be based on a variety of factors including, but not limited to, an economic value of the information, use or purpose of the information, number of users, and the availability from other sources. The tracking entries may also include additional data so that the information owner may determine who transferred the information, the amount of information transferred, type of transfer, i.e., rental for specified period of time, and the time of transfer. Tracking entries, in one embodiment, are recorded for all transfers, i.e., IP Bank 302 to cartridge 374 and

central information bank 100 to IP Bank 302. Utilizing these entries, an information owner may also determine the type of information that is being transferred, the number of transfers, and the identification of the information receivers. For example, the information may be used to determine whether targeted users are receiving certain promotional materials are being received by targeted users, or to determine responses to different information pricing strategies.

D. Encryption

The above-described point-of-sale delivery systems have the capability of performing dynamic encryption of data as the data is downloaded onto a user's storage medium. Dynamic encryption refers to the process in which the IP Bank works together with the storage medium to perform a proprietary encryption of downloaded data. In one embodiment, different levels of encryption are utilized based on a series of factors or variables. These variables include, but are not limited to, an economic life, a market value, a general availability, a replacement cost, time sensitivity, and potential number of users, of the information. For example, today's TV listings may have a low level, or complexity, of encryption as a result of the low market value, low replacement cost, and general availability from many sources. Conversely, a multi-volume legal treatise may, for example, have a high, or complex, level of encryption as a result of the limited availability, replacement cost, and long economic life of the information. Based on the described factors, a source, i.e., publisher, of information may decide the appropriate level of encryption for each portion of information from the initial transmission to central information bank 100 to a user's cartridge 374. The level of information encryption, in any location, i.e., bank 100, may be higher or lower than another location, i.e., cartridge 374. More specifically, each time information is downloaded, or transmitted, the level of encryption may be independently altered, or determined. For example, the level of encryption at central information bank 100 may be different, i.e., higher or lower, than the level of encryption of an IP downloaded to a user's cartridge 374.

In addition to dynamic encryption, other encryption may be performed as illustrated in Figure 12. Figure 12 illustrates a three level encryption process. For example, prior to transmitting information on the network, the data may be encrypted. This facilitates preventing unauthorized users from accessing the transmitted information on the network. In addition to the pre-transport encryption, the data, may be encrypted prior to being placed in an IP bank. Publishers or other owners of the information may have approval authority over this level of encryption to provide such information owners with satisfaction that the data is adequately protected.

Once the data is stored in the IP bank, dynamic encryption techniques may be used when downloading the data onto storage media. The storage medium (Figure 7) includes a proprietary environment for building, reading, viewing and processing. The medium also has a commercial operating system environment for processing information files. An information file directory registry forms a part of the proprietary application, and a file directory pointer is contained in the operating system application.

The dynamic encryption process, in one form, uses the permanent serial numbers stored in the storage medium, the user's personal identification number, a personal signature code number, and a password to further encrypt the data stored in the IP bank as the data is downloaded to a user's storage medium. The personalized variables and codings are combined with various individualized information file variables to form an individualized data structure for the data downloaded to the user's personalized medium. As a result, those information files are individualized pertaining to the medium, the version of software, the information file itself, and other variables.

The dynamic encryption assists in reducing the possibility of the unauthorized use of proprietary or other information by causing all information downloaded through the point-of-sale delivery system to be readable and accessible by a selected number of user readers/computers. Specifically, data storage medium

accessible from one reader/computer will not be accessible using another reader/computer unless such access has been prearranged such as by providing the other reader/computer with an identical user identification number and password.

Examples of well-known encryption algorithms which may used in performing the above described three level encryption include the Z8068 Data Ciphering Processor (DCP). The DCP contains the structure to encrypt and decrypt data using National Bureau of Standards encryption algorithms. It may be used in a variety of environments including in dedicated controllers, communication concentrators, terminals and peripheral task processors in general processor systems. DCP provides a high throughput rate using cipher feedback, electronic code IP or cipher block chain operating modes. The provisions of separate ports for key input, clear data and enciphered data enhances security. The host system communicates with the DCP using commands entered in the master port or through auxiliary control lines. Once set up, data can flow through the DCP at high speeds because input, output and ciphering activities can be performed concurrently.

In alternative embodiments, encryption and decryption may be performed in dedicated hardware and/or software functions. For example, each reader and cartridge 374 may include a dedicated encryption integrated circuit (IC) and a dedicated decryption IC to maximize the transfer speed of the information. The level of encryption and decryption may be altered by adding additional functions and by enabling or disabling the additional levels.

With respect to dynamic encryption, the following describes one of many methods of dynamic encryption that could be used. Particularly, each regularly used alpha or numeric symbol is assigned a corresponding number as illustrated in Table 1.

Table 1

symbol	A	B	C	D	E	F	G	H	I	J	K
code	1	2	3	4	5	6	7	8	9	10	11
symbol	L	M	N	O	P	Q	R	S	T	U	V
code	12	13	14	15	16	17	18	19	20	21	22
symbol	W	X	Y	Z	0	1	2	3	4	5	6
code	23	24	25	26	27	28	29	30	31	32	33
symbol	7	8	9	.	,	;	:	+	-	x	
code	34	35	36	37	38	39	40	41	42	43	44

The serial number stored on the cartridge would be used to determine how many slots the code should shift to the left at the start the encrypting. For example, if the serial number ended with six, before starting of encryption, the code would be shifted to the left by six places. Table 2 illustrates the code table after the shift.

Table 2

symbol	A	B	C	D	E	F	G	H	I	J	K
code	7	8	9	10	11	12	13	14	15	16	17
symbol	L	M	N	O	P	Q	R	S	T	U	V
code	18	19	20	21	22	23	24	25	26	27	28
symbol	W	X	Y	Z	0	1	2	3	4	5	6
code	29	30	31	32	33	34	35	36	37	38	39
symbol	7	8	9	.	,	;	:	+	-	x	
code	40	41	42	43	44	1	2	3	4	45	6

The selected user password then is used to determine after how many symbols the code should again shift to the left. As an example, if the password were ROSE, then using the codes from Table 2, the numeric statement for rose would be 24212511. When the corresponding numbers are added together until reaching, a number between 1 and 10, the number reached in our example is 9 [18.9]. So after every 9th letter, the codes would be shifted another 6 spaces to the left. After the encrypting of 9 letters, the codes would be set as set forth in Table 3.

Table 3

symbol	A	B	C	D	E	F	G	H	I	J	K
code	13	14	15	16	17	18	19	20	21	22	23
symbol	L	M	N	O	P	Q	R	S	T	U	V
code	24	25	26	27	28	29	30	31	32	33	34
symbol	W	X	Y	Z	0	1	2	3	4	5	6
code	35	36	37	38	39	40	41	42	43	44	1
symbol	7	8	9	.	,	;	:	+	-	x	
code	2	3	4	5	6	7	8	9	10	11	12

Because the fact that the encrypting tables are constantly shifting, under this simple method, the phrase "My brown dog has fleas." would be encrypted as follows:

19 31 6 8 24 21 29 20 6

16 27 19 12 20 13 31 18 24

23 19 37 11

Decoding using only Table 1, the coded phrase would read as follows:

S 4 F H X U 2 T F

P 0 S L T M 4 R X

W S . K

Without knowing other information, it would be very difficult to find a pattern that would allow one to decode the symbols.

Knowing the placement of the codes relative to the symbols at the start of the encryption process and the number of symbols between shifts, decoding an encrypted phrase is simply a reversal of the process applying each of the tables in reverse.

There are any number of other methods of dynamic encryption that use different methods to vary encryption codes as one proceeds through the data to be encrypted. The objective, of course, is to make decoding difficult by avoiding obvious patterns associated with conventional language and number usage, so one would simply select a suitably difficult to decode dynamic encryption method.

In another embodiment, the unique dynamic encryption and decryption algorithms and formulae are generated using a unique combination of the personal signature (identification number) of the user, the serial (registration) of the storage medium and the registration number associated with the master data file being copied and encrypted using commercially available encryption programming or services. The electronic copies of the encryption and decryption formulae so generated are then stored at the central information storage facility for later use. With this embodiment of the invention, a unique set of encryption and decryption algorithms or formulae are so created for each separate copy of IP file requested. A copy of the unique decryption algorithm and formula is stored on nonvolatile memory on the cartridge (user storage medium) for later use. The nonvolatile memory on the cartridge (user storage medium) is so encased and configured that any attempt to read data stored thereon in an unauthorized manner will cause the memory to become totally unreadable and unusable. The unique encryption algorithm and formula so created are used to dynamically encrypt the selected IP file as the file is being copied and downloaded to the user cartridge (user storage medium) for storage and later use.

At the same time, a unique electronic header file is created for association with the encrypted copy of the requested IP file. The header file contains the user registration information, the rules and restrictions on use of the encrypted requested IP file and the electronic address for finding the appropriate decryption algorithm and formula and the location of the applicable CCS for decryption and use of the data within the encrypted IP file. After generation, the header file is wrapped within the encrypted IP file as the dynamically encrypted file is being generated, is attached to the electronic copy of the encrypted file as a separate part, or is written as a separate distinct data file that is electronically linked to the encrypted IP file. The manner in which the special header file is attached to the encrypted IP file depends upon the desired level of security and the hardware configuration.

E. Tamper Protection

In one embodiment of the present invention, access to the information is monitored, or recorded, to determine attempted unauthorized access to the information. If an unauthorized access is recorded, or stored, onto a user's medium, for example cartridge 374, the next time that user attempts to download additional information to cartridge 374, an unauthorized access message may be transmitted to notify the appropriate party, for example the cashier. As a result of the unauthorized access message, the cashier may revoke user's cartridge 374, notify the proper authorities, or record an entry into the user's account for future action. More specifically and in one embodiment, the unauthorized access is determined by first reading, or recording, the specific identification data from the information requester, or receiver. If the data provided by the information receiver is determined to not match, i.e., is unequal, predefined values, the unauthorized access message is recorded and information exchange is prevented. The data determination may be completed using known comparison hardware and/or software functions.

Additionally, the unauthorized access message may be generated if a user having an incorrect purpose, or authorization code, attempts to access

unauthorized information. For example, in a corporate environment, if a user attempted to access information for which the user did not have the proper authorization code, an unauthorized access message is generated and may be sent to, for example a system administrator or a security official. Different level of unauthorized access messages may also be generated. For example, a high level message may be generated if a user attempts to decrypt the information stored in various locations within the system, for example IP Bank 302 using an unauthorized device. A lower level message may be generated if a remote user has attempted to access data that is one level above that user's authorized level.

G. Other Embodiments

In another embodiment, IP Bank 302 may be configured to capture and exchange real-time information. For example, as a professor presents material to students in a classroom, the professor's presentation may be captured and converted into copyrighted text and exchanged with remote users. This conversion may be completed using known voice to text conversion systems using a known computer system. The professor's presentation may be supplemented with previously prepared, or concurrently prepared, written text. The text may be digitized and properly integrated into the text using known methods. Remote users may receive information from the professor's lecture in real-time as the material is presented or may receive the information at a later time. Remote users receive only that information which the remote user is authorized to receive from IP Bank 302 as described above.

In yet another embodiment IP Bank 302 is configured to receive audio, video, and/or computer software code. For example and in one embodiment shown in Figure 13, IP Bank 302 is coupled to a Video Cassette Recorder (VCR) 600, a stereo system 610 including a cassette recorder/player 620, a Compact Disk (CD) or DVD-X player and/or recorder 630, a television 640, and a computer 650. As described above, authorized information is received from IP Bank 302, and in one embodiment is stored to a storage device, for example a memory device 660. The

memory device 660 may be a plurality of memory cells, for example Read Access Ram (RAM), Read Only Memory (ROM), a rotating storage unit, i.e., a hard disk, a magnetic storage medium, i.e., magnetic tape, or other storage media, for example an optical storage medium. After the remote user has selected the appropriate information to receive from IP Bank 302, the information is stored in device 660. Device 660 is configured to transfer the stored information to the selected playback device, i.e., Video Cassette Recorder (VCR) 600, stereo system 610, cassette recorder/player 620, CD or DVD-X player/recorder 630, television 640, or computer 650. For example, in one embodiment, the remote user downloads, or receives, the entire contents of a top ten music album. The contents of the album are stored in device 660. As described above, the information may be permanently stored or may be stored for a fixed period of time or number of uses. After downloading the information to device 660, the remote user may transfer the information to stereo system 610 for listening. In another embodiment, the information may be transferred to, or through, device 660 to one of the other components, i.e., cassette recorder 620, VCR 610, CD or DVD-X recorder 630, or computer 650. To limit unauthorized copying or playback, the information may be playback using only those components, i.e., cassette recorder 620, VCR 610, CD recorder 630, or computer 650, coupled to device 660. For example, the remote user may download a feature movie by saving the movie on a tape using VCR 610. The remote user may then playback the movie as authorized as long as the tape is playback in VCR 610 that is coupled to device 660. Similarly, the remote user may download a software program so that the information is stored in device 660 or in a storage medium in computer 650. Depending upon the authorization code of the software, the program may be configured to execute only from computer 650 when computer 650 is coupled to device 660.

The above-described system facilitates controlled and monitored exchange of information between many types of information owners, distributors, and users. By using the described system, a user may obtain many types of authorized information. The user may, as determined by the information owner, purchase, rent,

or obtain without charge, the authorized information. The information, in one embodiment, is encrypted using various levels, or complexities, of encryption to prevent unauthorized access. The level of encryption depends upon a variety of factors or variables, for example, the economic life of the information. For example, IP Bank 302 may include information representing a reference dictionary and a top ten music album. Information from the reference dictionary and the album may have the same or different levels of encryption. In addition, students from a determined class may access the reference dictionary information without charge as the result of the school purchasing an unlimited use copy of the information, however, those same students would be required to purchase any information downloaded from the album. Additionally, the type of access may differ for different portions of the information. For example, a first track of the album information may be coded so that anyone may download the information without charge, however, the remaining tracks of the album information may be coded to require payment to download.

In still another embodiment, and referring to Fig. 14 and Fig. 15, the present invention relates to a storage and retrieval system that is vendor, product, and IP independent. This embodiment provides an object-based system that packages any type of data on a network. The type of data in the package is immaterial to this embodiment. However, accurate, timely, and secure delivery is ensured by the facilities provided by this embodiment of the present invention. Each separate IP is stored in digital form, and a consistent interface is used for its delivery. Various levels of standardized encryption are available. IP so encrypted is distributed and read in a uniform manner.

One of the facilities provided is one or more central data centers or central data storage facilities 100. Each central data center 100 acts in conjunction with any others present in the network to store and control delivery of IP from IP content providers 707. In some embodiments, additional data centers 702 are provided, each comprising one or more computers acting in conjunction with each

other. Computers 704 need not be in the same location. Each data center 702 either services one or more local clients 706 or acts as part of central data center 100.

Local public devices, or kiosks 708, are networked to and controlled by the data center. Kiosks 708 are examples of interfaces or access ports by which consumers have access to central data center 100 and by which they acquire desired IP's. Besides kiosks, other examples of access ports are computers (mainframe, desktop, and laptop), personal digital assistants (PDAs), electronic books or ebooks, modems, and other devices designed for accessing electronic networks such as telephone, Lansat, Internet, intranet, and cable networks for electronic transfer of digital data.

A security encryption compression (SEC) module 710 is provided in each consumer product or user device 712 to control access to, and use of IP's. To obtain an IP, a consumer must have a registered SEC module 710 and an authentication password that is recognized by kiosk 708. In addition, the consumer must have a data storage medium 714 to hold a requested IP after downloading. SEC module 710 will securely store the IP for use in an appropriate manner. SEC module 710, in one embodiment, provides its own user interface (for example, a screen and/or speakers, etc.). In another embodiment, SEC module 710 provides one or more external adapters 716A, 716B, to provide a signal for display by one or more other user devices 712A, 712B, 712C, 712D. External devices 712A, 712B, 712C, 712D, communicate with SEC module 710 through, for example, infrared ports, RCA plugs, headphone jacks.

SEC module 710 provides security through an "onion" approach, i.e., one that is made up of multiple protection layers that surround the IP. A first such layer is a hardware layer. SEC 710 comprises, in one embodiment, a chipset having a unique serial number, nonvolatile random access memory (NV-RAM) 718, read-only memory (ROM) 720, and a programmable logic controller/processor 722 with electrically erasable programmable read only memory (EEPROM) 724. The unique

serial number provides part of a public/private encryption key along with a user's access code stored in NV-RAM 718 and the IP being accessed. Each IP is specifically encoded to work only with a specified piece of registered hardware accessed by a specific user's security code. For some IP products and in some embodiments, transfer from one SEC module 710 to another is possible, but only through an authenticating interface such as a kiosk. Hardware protection provided by SEC module 710 is also the first authentication required by the network before it permits IP to be exchanged. If an SEC module 710 is bypassed to obtain direct access to storage medium 714, the physical interruption is archived and transmitted to the network during a subsequent communication, for example, the next communication.

A second layer of security is provided by SEC 710 firmware. This layer is provided by a programmed EEPROM 724 that decrypts stored IP flowing to an output device. Public/private key encryption is dynamically controlled by each IP. In one embodiment, this control is monitored as well as modified each time SEC module 710 communicates with the network.

A third layer of security is in the IP itself. It is encrypted and compressed while downloading to storage medium 714 in an SEC module 710.

Information obtained from a participating publisher 707 in digital form is enveloped with a uniform electronic signature that uniquely marks the version, creating a master copy for distribution. The signed master copy is then encrypted using a custom encryption algorithm and stored in a centralized data storage facility 100 or facilities (depending upon the size of the distribution network) for later retrieval. Each stored work has a title, which is added to a master table of contents or index 726.

Central storage facility 100 is electronically accessed by a user via an access port using secure, encrypted application-layer protocols. These protocols are independent of network transport and physical layer protocols, and thus, usable on any transmission network. Utilizing these application-layer protocols, the user

communicates with and receives instructions from central storage facility 100 for acquiring an electronic version of one or more selected IP's. In preparation for downloading the selected IP's, central storage facility 100 further encrypts 728 the IP's selected for distribution in accordance with a level of encryption selected by the publisher of the IP.

Encryption is provided in several different forms. For example, public/private encryption keys are used for data storage. Watermarking is used when sending data to an unsecured device such as a headphone, a television set, or a word processor. For example, a watermark code is injected by a digital-to-analog (D/A) converter into an analog output signal, which, when analyzed, identifies a source of the IP and its purchaser or licensee. The D/A converter code is determined by the serial number and personal ID code in NV-RAM 718 and from coding in the IP itself, thereby uniquely identifying a combination of user, device, and IP. The secure transfer of IP from the network is done, for example, via RSA encoding, which is described in detail in U.S. Patent No. 4,405,829. This secure transfer ensures that each packet is uniquely encrypted as well as monitored for possible hijacking and other data stream tampering.

In this embodiment, compression is provided both to maximize storage capabilities and to provide another layer of security for the IP.

SEC 710, in one embodiment, is an integrated storage device, with at least one of a hard disk, a RAM disk, an NV-RAM card (e.g., a compact flash memory card) or other storage medium as medium 714. One or more interfaces 716A, 716B, 716C, 716D are provided between the integrated storage device 714 and one or more output devices 712A, 712B, 712C, 712D. SEC 710 is designed to permit storage device manufacturers to incorporate the chipset into their storage devices, so that the storage devices can accept IP from the network.

In one embodiment, SEC 710 comprises a storage medium 714, an SEC chipset 718, 720, 722, 724, a USB (universal serial bus) port 730 to interface

with a kiosk 708 for IP transfer, an A/D converter 716A, and a headphone jack 712A. Another embodiment provides both a USB and a USB2 connection. In yet another embodiment, SEC 710 includes a infrared (IR) port and an RCA jack. In still other embodiments, SEC 710 is built into a device such as a personal digital assistant (PDA) or a single-function reader that serves as a device for reading digital IP or ebooks. In yet another embodiment, SEC 710 is built into a user device such as a laptop or desktop computer. For example, half of the hard drive of the computer can be set aside for a traditional operating system and the other half dedicated for storing IP, for example, user video, books, and audio. Still other embodiments include other wireless couplings, iLink, Firewire, and/or IEEE 1394 connections, for example.

Encryption ensures protection for IP by allowing downloaded IP to be read only on a particular SEC 710, and only by a user knowing a particular password. This limitation is provided, for example, utilizing a decryption formula provided by a key generation company 732 such as Verisign, Inc. The key generation company creates a formula that enables a decryption key to reverse the encryption 728 provided the network. This formula is sent during registration of an SEC module 710 and burned into NVRAM 718 or other limited access memory in one embodiment. In another embodiment, the formula is preprogrammed into SEC module 710. In one embodiment, the formula is stored in an encrypted form and decrypted by SEC 710 hardware only while it is being used. In one embodiment, the same formula is used by the network to encrypt IP at the central data center and by SEC 710 to decrypt the encrypted IP, using different keys determined by key generation company 732.

In one embodiment of the present invention, modern algorithms and appropriate key lengths are used to protect the IP when an IP file is initially created, during its distribution, and throughout its existence. In addition, system programming regularly and automatically updates and changes encryption and decryption code algorithms, keys, and formulae both to recapture IP for which such protection has been broken or compromised and to inhibit the cracking or compromising of IP protection. The frequency and/or number of times that algorithms, keys, and/or

formulae are changed depends, in one embodiment, on one or more factors such as the length of time a user has rights to an IP, a level of security that is assigned to the IP, and a preassigned schedule that is based upon the level of security assigned to the IP.

Employing key generation company 732 independent of the network operator to generate keys is not necessary, but may be preferred by owners of IP who believe that extra security and accountability is provided by such companies. It is not necessary to employ the services of a key generation company, however. Thus, in one embodiment of the present invention, key generation facilities are provided within the network itself.

In one embodiment, operation of the network proceeds as follows. Digital IP of various types and from various sources 708 is obtained and stored at central data center 100. Users (or potential users) of the digital IP obtain a SEC module 710 with a unique serial number (USN) permanently "burned" into the electronics of the module. Each user also chooses a personal password (PP) to identify himself or herself for registration. The user-selected PP, in some embodiments, is constrained within limits selected for security and practicality by the network operator. For example, in one embodiment, the PP is constrained to be no less than 6 characters and no more than 12.

A user with an SEC module 710 and a selected password then connects SEC module 710 to a kiosk 708 or other access port. SEC 710 transmits the USN and the user-selected PP to the network for registration, where the USN and PP are combined (for example, by concatenation or by a mathematical or logical operation) into a unique code (UC). In at least one embodiment, the UC is sent to a key generation company 732, for example, Verisign, Inc. The network itself also generates a hidden private key (HPK) and sends it to key generation company 732. Key generation company 732 then computes a private encryption key (PEK) from the HPK and the UC and sends the PEK to the network, where it is used for encryption of IP as it is sent to the user of SEC 710. The user then enters the PP into SEC 710,

where it is combined with the USN (as combined by the network) to decrypt the IP for the user.

In one embodiment, servers 734 at the centralized storage facility or facilities 100 determine a most efficient cost effective path to distribute IP, including, but not limited to, books, music, video, computer software and multimedia, and automatically tracks, verifies end user tampering, freezes the end users access, and regulates distribution method requirements. The regulation varies for each account and industry. For example, a retail establishment will use a different set of rules requiring different distribution limitations, retrieval and viewing methods, and security and encryption specifications when distributing IP than an institution or an individual is likely to require. Also, methods of electronic distribution and security requirements vary in accordance with the types of IP that are distributed. For example, digital music transfer and retrieval is performed differently from digitally retrieving, and reading an electronic IP, or transferring, retrieving and viewing video. A portion of the verification programming is devoted to checking and verifying the readability of the IP file after being encrypted and downloaded to the user's storage medium. The verification programming also attempts to correct correctable errors automatically and indicates detectable, but uncorrectable, errors. If uncorrectable errors are found during verification, the downloading and encryption process is repeated for a predetermined number of times or until no uncorrectable errors are detected within the predetermined number of attempts. If uncorrectable errors remain after the predetermined number of attempts is exhausted, the user is directed to a service representative to provide assistance. In one embodiment, CCS is also programmed or otherwise configured to automatically verify the readability of an encrypted IP during access for reading and automatically attempts to correct any errors discovered that do not relate to functioning of the security mechanism. For example, CCS is programmed to detect and correct errors resulting from media deterioration. Such errors can result from passage of time or from repeated access or use.

In one embodiment, the current invention consolidates distribution all forms of IP into one network that is transparent to the end consumer. The network includes transparent links that feeds to various IP web-sites 736 requested information. When an end user orders IP works via a web site 736, central repository 100 storing the requested data links the request and transmits the IP to a user's computer 738 (or other apparatus) with a secure dynamic encryption code that adds another layer of security to the secondary repositories. Participating IP retailers' web sites, kiosks, or other terminals, depending upon the needs of particular retailers, are also transparently linked to the centralized repository. Thus, a retail customer can continue to purchase IP content from a favorite retailer's web site or store, while the retailer links to the central IP data repository "behind the scenes."

Depending upon the most efficient and cost effective distribution method, the one or more centralized repositories 100 are locally based, regionally based or centrally based. Each central repository tracks IP data and credits sales 740, 742 to retailer sites. Key locking is provided so that individual retailers have access to their own sales tracking information at the central depository, irrespective of whether sales transfers occurred via Internet, microwave, infrared, satellite, cable, telephone, or other medium.

One embodiment of the present invention is linked to various web sites 736 in a manner transparent to consumers. When purchases are made through various web sites, stores or organizations, corporations, etc., an earmarked transactional fee is tracked, accounted for, and distributed to that particular entity through a universal tracking system 740, 742. In this embodiment, the central information storage facility is a grouping of separate servers or storage facilities at one or more physical locations that are physically operated by one or more persons and that are linked together via a network arrangement and by appropriate software such that they appear to the user to be a single functioning storage facility. Retail companies are thus provided with income, irrespective of whether their customers receive downloaded IP products via a web site 736 of the retailer, from a high-bandwidth kiosk 708 at a traditional store, or

recorded on media by the retailer on demand at a retail establishment. Using this embodiment of the present invention, retailers can provide a useful, profitable service by distributing IP through in-store kiosks or on media recorded by the retailer on demand to customers lacking high-speed Internet connections. Providing this service may be a decisive advantage to some retailers. The additional flexibility afforded retailers by the present invention may also help retailers avoid market base erosion as Internet bandwidth to the home continues to expand.

In one embodiment, IP's and/or links to IP's (i.e., pointers to another location where the IP is stored, such as on a server of an IP content provider 707) are obtained from content providers 707. Referring to Fig. 16, when IP is stored 800, a format conversion 1001 is performed. Format conversion 1001 includes "system encryption," so that the IP is unreadable on other systems. When a request is received, personalized encryption 1002 is applied, followed by dynamic encryption 1003 as the IP is transmitted over a network 804. (Encryptions 1002 and 1003 are configured so that they can be performed at essentially the same time, even though a temporary storage 802 is shown between them.) In the case of an IP link, format conversion 1001 is triggered by a user request. The result is stored in a temporary storage 812 (rather than a permanent storage in central data center 100, as is the case when the IP is stored, rather than linked). Personalized encryption 1002 and dynamic encryption 1003 is then applied before transmission over network 1003. (Temporary storage 814 is not necessarily different from temporary storage 802.) As the user downloads the IP, it is stored in user storage 714, where decryption of encryption algorithms 1003, 1002, and 1001 are performed, in the reverse order to which the encryption 1001, 1002, 1003 were applied. Decryption 1002 is performed from temporary storage 806 into a secure RAM 808, using SEC 710. The content of secure RAM 808 is displayed 810, after encryption 1001 is decrypted. Storage 806 and 808 are erased when the IP is no longer needed. User storage 714 is also erased under some conditions, such as when tampering is detected.

The registration, security, tagging (or watermarking), verification and use analysis programming produces a data trail logging the creation and use of a particular IP file by a user, thereby providing evidence of accountability in the event of an actual or attempted breach of the security features associated with the IP file. The registration, security, tagging verification and use analysis programming creates a permanent linking of a given copy of an IP file to a user requesting its creation and a user device used to create the copy in question. A permanent log of use of the IP file, in digital form, is stored in a separate memory storage area associated with the CCS programming and a copy of the log is periodically transferred to the central information data storage facility for storage and later analysis.

As illustrated in Figure 1, in one embodiment of the invention, security is enhanced through the use of an external authentication device [302A] affixed or connected to the user's device and a related identifier. Examples of suitable, currently available external authentication devices include parallel port software locks, iButtoms[tm] (Dallas Semiconductor Corp. of Dallas, TX) and "Smart Cards" plugged in via a pc-card. In such embodiment, upon registering a user is physically given an identification code disk, card or button that is encoded with user identification information that is electronically readable when the code disk, card or button is inserted in an appropriate slot associated with the external authentication device. If the externally inserted electronic identification codes match the required codes for access, access to the encrypted files is allowed. If the externally inserted electronic identification codes do not match the required codes for access, access is denied.

In yet other embodiments of the present invention, user device 712 is a cellular or other wireless mobile telephone or wireless communications unit, for example, a cell phone with a wireless browser. With this type of user device, IP text can be downloaded directly to the wireless communications unit via the appropriate cellular or other type of wireless mobile network. In one embodiment, for example, the IP text is written text, pictures, or other visual content that is displayed in a browser window. In another embodiment, the IP text is music that is downloaded

directly to a cellular or other wireless mobile telephone. (One embodiment of a wireless telephone useful for this invention includes stereo headphones, or has a jack for such headphones.) The IP text undergoes dynamic encryption, as in other embodiments of the invention, and is decrypted, but not stored in the telephone or on other media. When a call is received, an audible or other type of indication is provided on the wireless telephone user device 712, and the music is interrupted when the call is answered. In yet another embodiment, music is selectively streamed to headphones or speakers, saved to a recording medium in the wireless telephone user device 712, or both. Telephone 712 is configured so that the music can be selectively saved via downloading to the recording medium when a call interrupts music being streamed for listening.

It will thus be seen that one or more embodiments of the present invention provide one or more IP consolidation features such as overall "mothership" IP encryption, open web selection and browser access, user screening ID and control, transfer verification, transaction purchase, attachment of secure rules, functionality and user allowances, auditing, and feedback and updating. While the present invention has been described with respect to specific embodiments, many modifications, variations, substitutions, and equivalents will be apparent to those skilled in the art. Accordingly, the invention is to be considered as limited only by the spirit and scope of the appended claims.

CLAIMS:

1. Apparatus for facilitating obtaining text of an IP, comprising:

a storage device having stored therein text of a plurality of IP, wherein the text includes electronically stored representations of at least one member of the group consisting of printed text works, movies, films, video presentations, television programming, music, audio works, audio presentations, radio programs, graphic material, art works, plays, operas, novels, writings, photographs, pictures, images, advertising copy, software, and portions and combinations thereof;

a processor connected to said storage device, said storage device further having stored therein a program for controlling said processor, said processor operative with the program to:

receive an IP selection request;

receive a user identification associated with the IP selection request; and

output encrypted text of the selected IP if the user identification and IP selection are valid utilizing a determined level of IP encryption.

2. Apparatus in accordance with Claim 1 wherein said processor is further operative with the program to purpose encode the text of the selected IP so as to limit a purpose which access by the user to the text is authorized.

3. Apparatus in accordance with Claim 1 wherein said processor is further operative with the program to encrypt the text of the selected IP utilizing an identifier associated with the user.

4. Apparatus in accordance with Claim 1 configured to electronically associate instructions provided by an IP supplier and relating to allowed

use, access, and pricing of IPs supplied by the supplier with the IPs supplied by the supplier.

5. Apparatus in accordance with Claim 4 further configured to receive use and access choices from the user associated with the IP selection request, and to use the instructions provided by the IP supplier and associated with the text of the selected IP to generate an electronic IP instruction file linked with the outputted text of the selected IP to regulate use of and access to the outputted text.

6. Apparatus in accordance with Claim 1 further configured to receive a determined level of security including the determined level of encryption from a supplier of the selected IP, the determined level of security being selected from a range of security levels.

7. Apparatus in accordance with Claim 1 wherein said determined level of IP encryption is based on at least an economic value of the selected IP.

8. Apparatus in accordance with Claim 1 wherein said processor is further operative with the program to encrypt the text of the selected IP utilizing a unique identification number associated with at least one of a user device and user data storage medium used to download or store the encrypted text of the selected IP.

9. Apparatus in accordance with Claim 1 wherein said processor is further operative with the program to cooperate with a user device being used to download and read a selected IP text, to restrict and regulate operation of the user device to limit reading and copying of the selected IP text.

10. Apparatus in accordance with Claim 9 wherein said processor is further operative with the program and the user device to determine whether IP texts downloaded to the user device have been used in an unauthorized manner, and to at least one of restrict or deny access to such IP texts when such unauthorized use is determined to have occurred.

11. Apparatus in accordance with Claim 10 wherein said processor is further operative with the program and the user device to cause the user device to permanently erase an IP text from memory of the user device when such unauthorized use is determined to have occurred.

12. Apparatus in accordance with Claim 9 wherein said processor is further operative with the program and the user device to cause the user device to at least one of temporarily restrict or deny access to an IP text in a memory of the user device.

13. Apparatus in accordance with Claim 1 further comprising at least one local unit communicatively coupled to said processor, said local unit comprising a memory for storing, in electronic form, information transmitted to said unit from said processor, and a local unit processor for controlling transfer of information stored in said unit to electronic storage media of system users, said local unit configured to encrypt the information when the information is to be transferred to the electronic storage media, said local unit configured to encrypt the information utilizing a determined level of information encryption.

14. Apparatus in accordance with Claim 13 wherein the information stored on a user's storage medium comprises a personal signature code number and serial number.

15. Apparatus in accordance with Claim 13 further configured to receive a determined level of security, including the determined level of encryption, from a supplier of the selected IP, the determined level of security being selected from a range of security levels.

16. Apparatus in accordance with Claim 15 wherein said determined level of information encryption and security is based upon at least an economic value of the selected IP

17. Apparatus in accordance with Claim 16 wherein the level of information encryption is not equal to the level of the IP encryption.

18. Apparatus in accordance with Claim 13 wherein the memory of the local unit is configured to regulate the use of information stored therein in encrypted or decrypted form so long as an electronic connection exists between the local unit and a user data storage medium, and to permanently erase selected files from the memory of the local unit whenever the electronic connection is no longer active.

19. Apparatus in accordance with Claim 1 wherein said processor is further operative with the program to determine attempted unauthorized access to the output copies of the text of an IP.

20. Apparatus in accordance with Claim 1 further configured to receive information identifying an establishment from which the IP selection request originated, and to tag the encrypted text of the selected IP with an identification of the establishment.

21. Apparatus in accordance with Claim 20 wherein said processor is further operative with the program to utilize the tag to trace IP text to an establishment.

22. Apparatus in accordance with Claim 1 wherein said processor is further operative with the program to determine and store information relating to usage of the encrypted text by the user and which will cause said usage information to be encrypted and stored in a segregated section of the memory associated with the user storage medium or local unit and which will cause said usage information in encrypted form to be transmitted to the central data storage facility when said local unit and/or user data storage unit are later electronically connected to the central data storage facility.

23. A method for operating a computer to obtain text of an IP, comprising:

inputting into the computer an IP selection request;

inputting into the computer a user identification associated with the IP selection request;

inputting a unique identification number associated with at least one of a user device or user storage medium being used to at least one of download or store an encrypted copy of a selected IP corresponding to the IP selection request,

generating a unique encryption algorithm and a corresponding decryption algorithm, using the user identification and at least one member of the group consisting of: (a) a digital identification number associated with at least one of the user device or a user data storage medium, and (b) a digital identification associated with the selected IP;

communicating encrypted text of the selected IP to the user device for storage on the user storage medium using the unique encryption algorithm for encryption, wherein text of the selected IP comprises electronic representations of at least one member of the group consisting of: printed text works, movies, films, video presentations, television programming, music, audio works, audio presentations, radio programs, graphic material, art work, plays, operas, novels, writings, photographs, pictures, images, advertising copy, software, and portions and combinations thereof;

generating a header associated with the encrypted text of the selected IP file that contains, in digital form, a user identification, an identification of at least one of the user device or user data storage medium one which the encrypted digital copy of the selected IP is to be stored, a usage authorization indication, and an electronic address of the corresponding decryption algorithm;

validating the user identification, authorization indication, and IP selection, after the unique encryption algorithm and corresponding decryption algorithm have been generated; and

decrypting the digitally encrypted text of the selected IP using the corresponding decryption algorithm, conditioned upon said validation.

24. A method in accordance with Claim 23 wherein inputting to the computer an IP selection comprises the steps of:

selecting at least one of the IP in the memory storage; and

selecting the text of at least a portion of each the selected IP.

25. A method in accordance with Claim 24 wherein inputting to the computer an IP selection further comprises the steps of:

determining if more than one portion of an IP is selected; and

if more than one portion of an IP is selected, then combining the selected portions.

26. A method in accordance with Claim 23 further comprising the step of generating tracking information corresponding to the selected portions and the selected IP.

27. A method in accordance with Claim 23 further comprising the step of purpose-encoding the encrypted text of the selected IP so as to limit a purpose for which access by the user to the text is authorized.

28. A method in accordance with Claim 23 further comprising the step of determining a level of IP encryption.

29. A method in accordance with Claim 28 wherein determining a level of IP encryption comprises the step of selecting at least one of a plurality of levels of encryption code.

30. A method in accordance with Claim 29 wherein the step of generating the unique encryption algorithm and corresponding decryption algorithm comprises the step of obtaining the unique encryption algorithm and corresponding decryption algorithm from an independent key supplier.

31. A method in accordance with Claim 30 further comprising the step of storing copies of the obtained encryption and decryption algorithms in a memory of a central information storage facility for later use.

32. A method in accordance with Claim 30 wherein the at least one of the user device or user storage medium has a write once, read many times (WORM) memory unit contained therein, the WORM memory being configured to become inoperable when unauthorized access thereto is attempted;

said method further comprising the step of storing a digital representation of the unique encryption algorithm and of the corresponding decryption algorithms in the WORM memory for later use.

33. A method for operating a processor communicatively coupled to a network to obtain text of an IP, the network being coupled to a memory storage having stored therein text of a plurality of IP wherein the text of an IP comprises electronic representations of at least one member of the group consisting of: printed text works, movies, films, video presentations, television programming, music, audio works, audio presentations, radio programs, graphic material, art work, plays, operas, novels, writings, photographs, pictures, images, advertising copy, computer games, video games, software, and portions and combinations thereof; said method comprising:

determining an IP selection request;

inputting into the processor the IP selection request;

inputting into the processor a user identification associated with the IP selection request;

inputting a unique identification number associated with at least one of a user device or a user data storage medium in which an encrypted electronic copy of the text of the selected IP is to be stored;

outputting encrypted text of the selected IP if the user identification and IP selection request are valid utilizing a determined level of encryption.

34. A method in accordance with Claim 33 wherein determining the IP selection request comprises the steps of:

reviewing the IP in the memory storage;

selecting the text of at least a portion of at least one of the IP in the memory storage.

35. A method in accordance with Claim 33 wherein determining the IP selection request comprises the steps of:

selecting at least one IP in the memory storage;

selecting the text of at least a portion of each selected IP in the memory storage;

combining the selected portions of the selected IP.

36. A method in accordance with Claim 35 wherein selecting the text of at least a portion of each selected IP in the memory storage comprises the step of selecting the entire IP.

37. A method in accordance with Claim 35 wherein selecting the text of at least a portion of each selected IP in the memory storage comprises the step of selecting at least one word of each selected IP.

38. A method in accordance with Claim 35 wherein selecting the text of at least a portion of each selected IP in the memory storage comprises the step of selecting at least one section of each selected IP.

39. A method in accordance with Claim 35 further comprising the step of generating tracking information corresponding to the selected IP in the memory storage.

40. A method in accordance with Claim 39 further comprising the step of generating tracking information corresponding to the selected portions of the selected IP.

41. A method in accordance with Claim 39 further comprising the step of generating tracking information relating to usage of selected IP relative to a retail establishment location.

42. A method in accordance with Claim 33 further comprising the step of purpose encoding the encrypted text of the selected IP so as to define a purpose of use which access by the user to the text is authorized.

43. A method in accordance with Claim 33 further comprising the step of determining unauthorized access to the encrypted text.

44. A method in accordance with Claim 33 wherein the step of outputting encrypted text of the IP comprises the step of generating a unique encryption algorithm and a corresponding decryption algorithm using the user identification and at least one member of the group consisting of: (a) the digital identification number associated with at least one of the user device or the user data storage medium, and (b) a digital identification associated with the selected IP.

45. A method in accordance with Claim 44 wherein the step of generating the unique encryption algorithm and corresponding decryption algorithm comprises the step of obtaining the unique encryption algorithm and corresponding decryption algorithm from an independent key supplier.

46. A method in accordance with Claim 45 further comprising the step of storing copies of the obtained encryption and decryption algorithms in a memory of a central information storage facility for later use.

47. A method in accordance with Claim 46 wherein the at least one of the user device or user storage medium has a nonvolatile memory contained therein, the nonvolatile memory being configured to become inoperable when unauthorized access thereto is attempted;

said method further comprising the step of storing a digital representation of the unique encryption algorithm and of the corresponding decryption algorithms in the nonvolatile memory for later use.

48. A method in accordance with Claim 45 wherein said step of outputting encrypted text of the selected IP comprises the step of using the unique encryption algorithm to encrypt a digital copy of the selected IP as the copy is being made and downloaded to a user's data storage medium.

49. A method in accordance with Claim 33 further comprising the step of outputting, in association with the encrypted copy of the selected IP, information from which at least one member of the group consisting of: (a) access authorization codes, (b) usage authorization codes, and (c) a decryption algorithm for decrypting the encrypted text of the IP can be determined.

50. Apparatus for facilitating obtaining text of an IP, wherein the text includes electronic representations of at least one member of the group consisting of: printed text works, movies, films, video presentations, television programming, music, audio works, audio presentations, radio programs, graphic material, art work,

plays, operas, novels, writings, photographs, pictures, images, advertising copy, computer games, video games, software, and portions and combinations thereof; said apparatus comprising:

a storage device having stored therein text of a plurality of IP;

a processor connected to said storage device, said storage device further having stored therein a program for controlling said processor, said processor operative with the program to:

receive an IP selection request;

receive a user identification associated with the IP selection request; and

dynamically encrypt text of the selected IP as the text is output from the apparatus, using an encryption algorithm.

51. Apparatus in accordance with Claim 50 wherein said apparatus is configured to communicate via a network connection selected from the group consisting of: electronic cable connections, wired connections, commercial telephone connections, commercial cable network connections, cellular and other wireless mobile network connections, infrared connections, microwave connections, radio wave and other wireless connections, television wave connections, local device generated infrared signal connections, laser connections, and connections allowing for transfer of data in digital form from one point to another, and combinations thereof.

52. Apparatus in accordance with Claim 50 wherein said processor is further operative with the program to purpose encode the text of the selected IP so as to limit a purpose which access by the user to the text is authorized.

53. Apparatus in accordance with Claim 50 wherein said processor is further operative with the program to access encode the text of the selected IP so as to regulate access to the encrypted selected IP.

54. Apparatus in accordance with Claim 50 wherein said processor is further operative with the program to receive instructions from an IP supplier relating to permissible use and access to IP texts supplied by the IP supplier, to associate said instructions with corresponding IP texts, to receive usage and access choices from the user in conjunction with the IP request, and to use said instructions associated with said texts to generate an electronic instruction data file with the requested IP, the instruction data file having instructions readable by a user device to regulate use of and access to the selected IP after it is downloaded and stored on a user device or storage medium.

55. Apparatus in accordance with Claim 50 further comprising at least one local unit communicatively coupled to said processor, said local unit comprising a memory for storing, in electronic form, information transmitted to said unit from said processor, and a local unit processor for controlling transfer of information stored in said unit to electronic storage media of system users, said local unit configured to encrypt the information when the information is to be transferred to the electronic storage media, said local unit configured to encrypt the information utilizing a determined level of encryption.

56. Apparatus in accordance with Claim 50 further configured to:

communicate, to a key generation service via a communication network, information relating to at least one member of the group consisting of: (a) a digital identification number associated with at least one of a user device or a user data storage medium, and (b) a digital identification associated with the selected IP; and

receive an encryption algorithm corresponding to the selected level of encryption from the key generation service via the communication network.

57. Apparatus in accordance with Claim 50 wherein said processor is further operative with the program to encrypt the text of the selected IP utilizing a

unique identification associated with at least one of a user device or a user data storage medium being used to download or store the encrypted text.

58. Apparatus in accordance with Claim 50 wherein said processor is further operative with the program to restrict and regulate the operation of a user device and user data storage medium that receives the encrypted text of the IP by restricting ability of the user device to perform at least one operation selected from the list consisting of: (a) printing of the IP, (b) copying of the IP, and (c) permanently storing decrypted text of the IP to another storage medium; and to cause selected information to be permanently erased from memory associated with the user device when a connection between the user device and a user data storage medium on which encrypted data files are stored is broken.

59. Apparatus in accordance with Claim 58 wherein said processor is further operative with the program to periodically change encryption and decryption algorithms and formulae associated with a copy of a selected IP text as a function of at least one of passage of time and use of the selected IP text.

60. Apparatus in accordance with Claim 50 wherein said processor is further operative with the program to receive a user-provided access code and generate a system access code, and to restrict and regulate access to encrypted text of the IP by encrypting text of a selected IP using the user-provided access code and generated system access code so that both are required to decrypt the text of the selected IP.

61. Apparatus in accordance with Claim 50 wherein said processor is further configured to receive, in encrypted form, usage and access information relating to a user device for reading electronic texts of IP when the user device is communicating with the apparatus.

62. A method for distributing intellectual properties (IP's) in digital form, said method comprising the steps of:

obtaining information from a plurality of publishers, the information being selected from the group consisting of IP's, links to IP's, and combinations of IP's and links to IP's;

encrypting IP's obtained from the publishers;

storing the encrypted IP's in a storage facility;

indexing the stored, encrypted IP's and links to IP's;

transmitting at least selected portions of the index to customers via a network;

receiving selective electronic requests for the IP's from the customers via the network;

transmitting requested IP's to customers in response to their electronic requests, including dynamically encrypting the IP's; and

recording transaction fees for the transmissions.

63. A method in accordance with Claim 62 further comprising the step associating an electronic signature personalized to a requesting customer with the IP's transmitted to the requesting customer in response to the requesting customer's request.

64. A method in accordance with Claim 62 further comprising the steps of:

maintaining an accounting of IP's transmitted utilizing the electronic signatures;

billing customers for IP's transmitted in response to their requests, and crediting publishers for publisher's IP's transmitted to customers.

65. A method in accordance with Claim 62 wherein the IP's include compilations of portions of IP.

66. A method in accordance with Claim 62 wherein the selective electronic requests for the IP's include requests for information available as IP links, and wherein transmitting requested IP's to customers, including dynamically encrypting the IP's comprises the steps of:

retrieving a copy of an IP corresponding to an IP link;

processing the copy of the IP so as to make it readable on a device of the requesting customer; and

dynamically encrypting the processed copy of the IP.

67. A method in accordance with Claim 62 wherein transmitting the requested IP's comprises the step of transmitting instructions to corresponding requesting customers for acquiring the requested IP's.

68. A method in accordance with Claim 67 wherein transmitting instructions for acquiring the requested IP's includes transmitting one or more instruction selected from the set consisting of: how to buy the requested IP's, how to rent the requested IP's, how to pay for the requested IP's, and how to read the requested IP's.

69. A method in accordance with Claim 67 wherein transmitting instructions for acquiring the requested IP's includes transmitting hardware and software requirements for reading the requested IP's.

70. A method in accordance with Claim 62 further comprising the step of encrypting at least one of the requested IP's with a customer-specific algorithm to allow the at least one requested IP to be read on more than one user device having an electronic identification associated with the customer.

71. A method in accordance with Claim 62 wherein transmitting the encrypted IP's comprises further encrypting the selected, encrypted IP's in accordance with a level of encryption selected by a publisher of the IP.

72. A method in accordance with Claim 62 wherein said step of receiving selective electronic requests for the IP's from customers via a network comprises receiving selective electronic requests from end users of the IP's via a public network.

73. A method in accordance with Claim 72 wherein the public network comprises the Internet.

74. A method in accordance with Claim 62 wherein said step of receiving selective electronic requests for the IP's from customers via a network comprises receiving selective electronic requests transmitted from network terminals located in retail establishments.

75. A method in accordance with Claim 74 wherein said step of receiving selective electronic requests transmitted network terminals located in retail establishments comprises receiving electronic requests sent by at least one member of the group consisting of: employees, proprietors, and combinations thereof, of the retail establishments.

76. A method in accordance with Claim 75 and further comprising the steps of maintaining an accounting of IP's transmitted utilizing electronic signatures personalized to requesting customers, and crediting IP sales to the retail establishments.

77. A method for uniform storing, encryption, and electronic distribution of digitized intellectual property (IP) comprising:

creating an electronic index of a collection of digitally-stored intellectual property;

generating authorization information unique to a user when the user accesses a central digital IP storage facility;

regulating access to digitized IP at the central storage facility to authorized users;

transmitting digitized IP from the digital storage facility to authorized users, including dynamically encrypting the digitized IP;

generating a unique registration number for each transmitted digitized IP associating the authorized user downloading the digitized IP and a user storage device receiving the transmitted IP.

78. A method in accordance with Claim 77 further comprising the steps of recording and storing, as a data file stored on a central data storage file, information identifying and relating users requesting transmission of a digitized IP with the requested, digitized IP.

79. A method in accordance with Claim 78 further comprising the step of providing access to the information identifying and relating the users to the transmitted digitized IP only to selected individuals.

80. A method in accordance with Claim 78 further comprising the step of indexing the information identifying and relating the users to the transmitted digitized IP in accordance with one member of the group consisting of: date, user, and digitized IP identification.

81. A method in accordance with Claim 78 wherein dynamically encrypting the transmitted IP comprises generating and attaching a time code tag indicating at least one of: (a) a length of time that access to a transmitted IP will be allowed, and (b) a time period that access to a transmitted IP will be allowed.

82. A method in accordance with Claim 78 wherein dynamically encrypting the IP comprises changing assigned encryption and decryption algorithms

for a transmitted IP stored in a user device or on a storage medium, said changing occurring in accordance with a function of at least one of use of the transmitted, stored IP, and time.

83. A wireless telephone communications device configured to:

communicate over a wireless network;

receive, decrypt, and play an interruptible, encrypted stream of music; and

to interrupt the stream of music when a call is received and answered.

84. A device in accordance with claim 83 further having storage for recording the stream of music.

85 A device in accordance with Claim 84 further configured to selectively record music into storage when the stream of music is interrupted.

86. A device in accordance with Claim 83 configured for stereo playing of the music stream.

87. A method for transmitting IP to a mobile station comprising the steps of:

obtaining information from a plurality of publishers, the information being selected from the group consisting of IPs, links to IPs, and combinations of IPs and links to IPs,

receiving selective electronic requests for the IPs from customers via a mobile, wireless network;

transmitting requested IPs to customers in response to their requests via the mobile, wireless network, including dynamically encrypting the IPs; and

recording transaction fees for the transmissions.

88. A method in accordance with Claim 87 wherein the IPs comprise at least one member of the set consisting of movies, films, video presentations, television programming, music, audio works, audio presentations, and radio programs; and wherein the step of transmitting requested IPs to customers comprises the step of synchronously transmitting requested IPs to customers.

89. A method in accordance with Claim 87 wherein the IPs comprise at least one member of the set consisting of movies, films, video presentations, television programming, music, audio works, audio presentations, and radio programs; and wherein the step of transmitting requested IPs to customers comprises the step of asynchronously transmitting requested IPs to customers.

90. A method in accordance with Claim 87 wherein the wireless network is a cellular network.

91. A method in accordance with Claim 87 further comprising the step of transmitting instructions with the requested IPs containing limitations pertaining to the use of the requested IPs by the customers.

92. A method in accordance with Claim 91 wherein the instructions include instructions pertaining to the autoerasure of the requested IPs.

PCT/US01/05706

device or on a storage medium, said changing
ction of at least one of use of the transmitted,

phone communications device configured to:

ireless network;

)lay an interruptible, encrypted stream of music;

of music when a call is received and answered.

:ordance with claim 83 further having storage for

:cordance with Claim 84 further configured to
when the stream of music is interrupted.

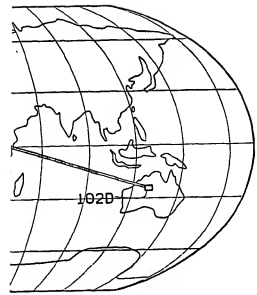
:cordance with Claim 83 configured for stereo

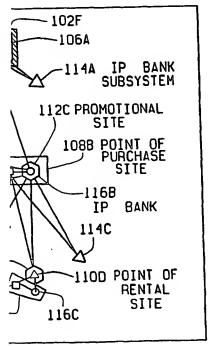
:ansmitting IP to a mobile station comprising the

from a plurality of publishers, the information
ing of IPs, links to IPs, and combinations of IPs

:tronic requests for the IPs from customers via a

IPs to customers in response to their requests
ıding dynamically encrypting the IPs; and





3 . 1

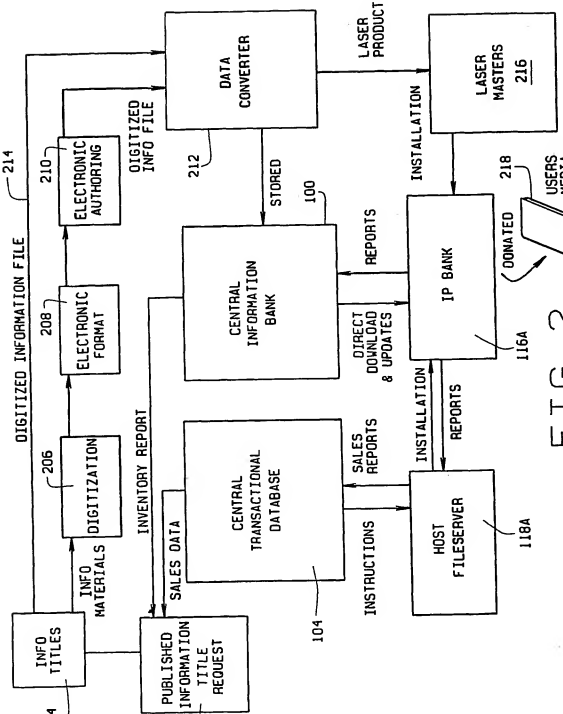


FIG. 2

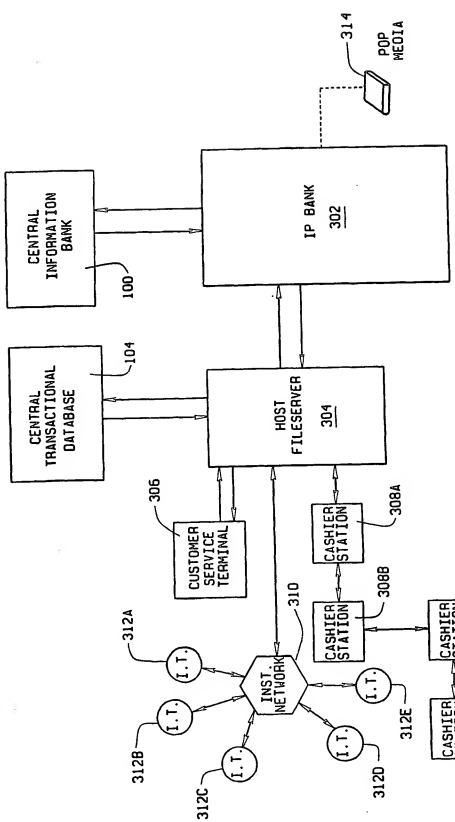


FIG. 3

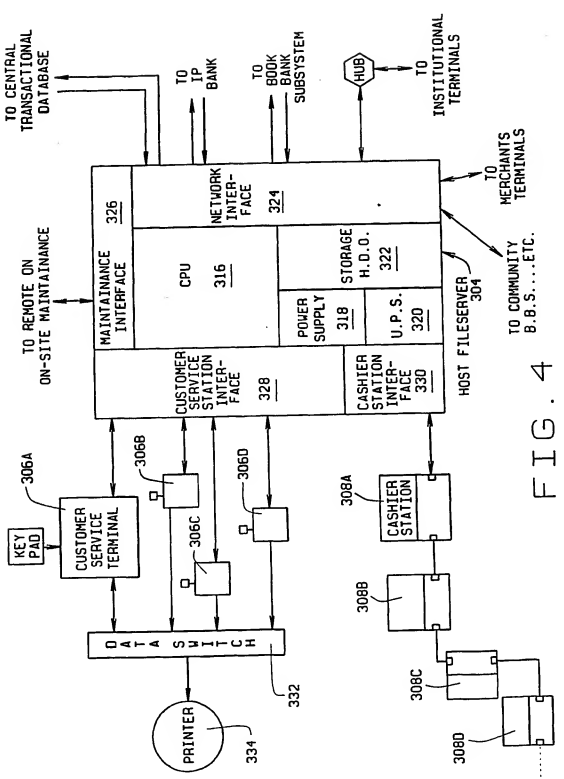


FIG. 4

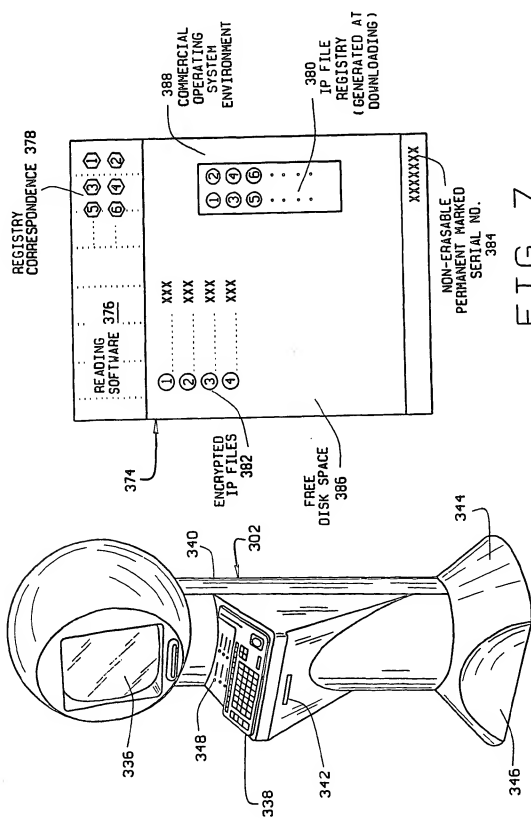


FIG. 5

FIG. 7

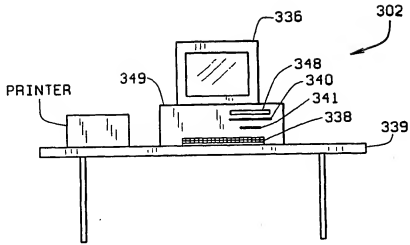


FIG. 5A

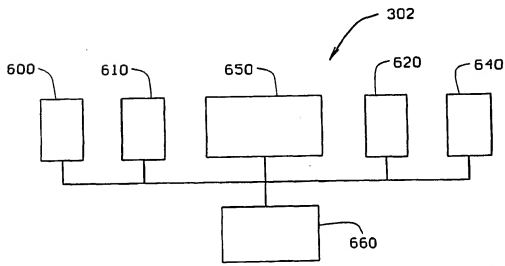


FIG. 13

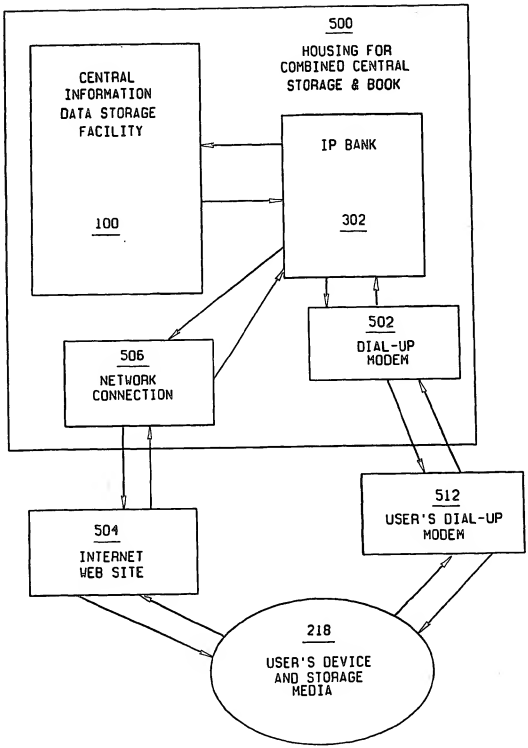


FIG. 5B

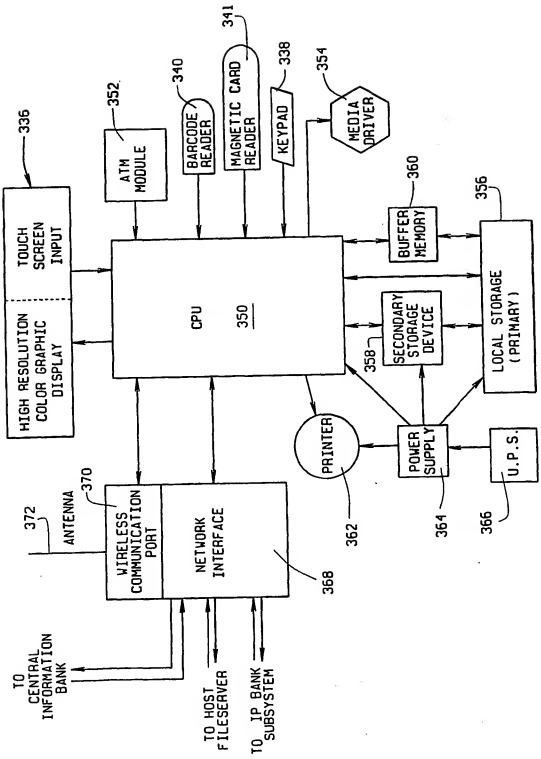


FIG. 6

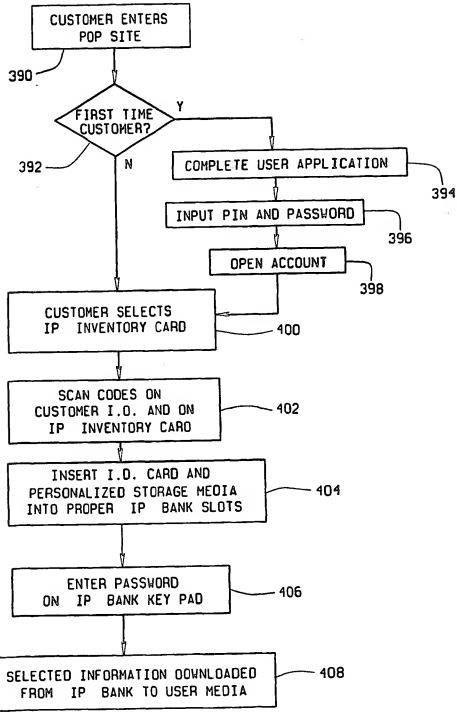


FIG. 8

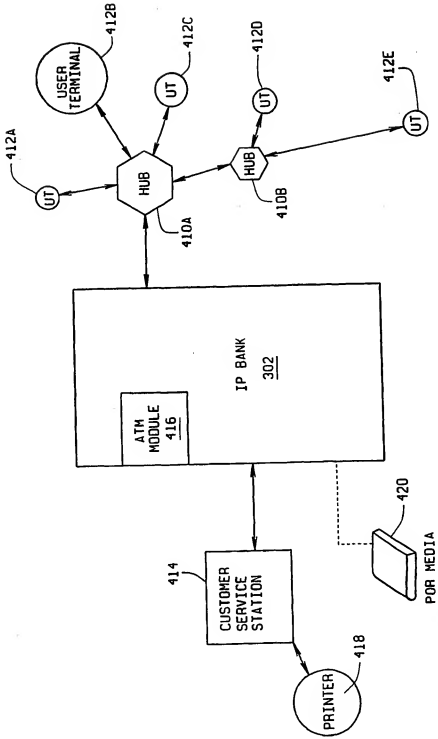


FIG. 9

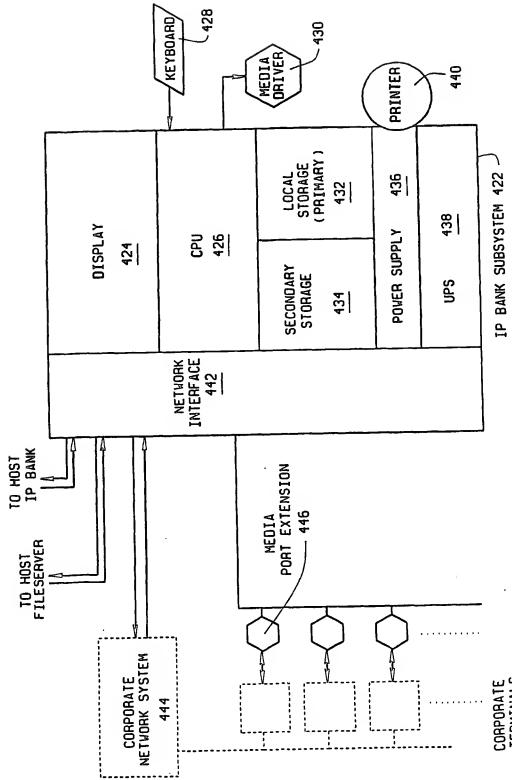


FIG. 10

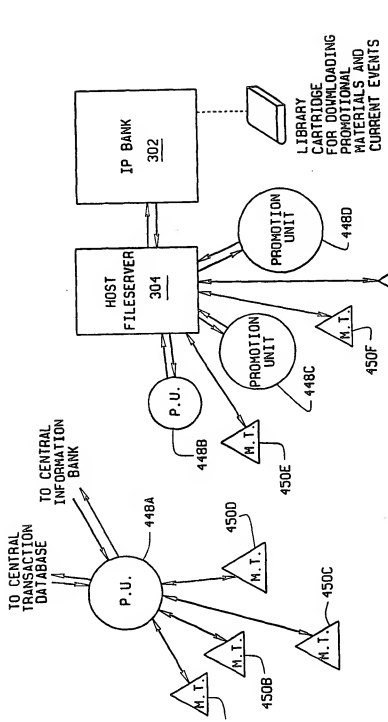


FIG. 11

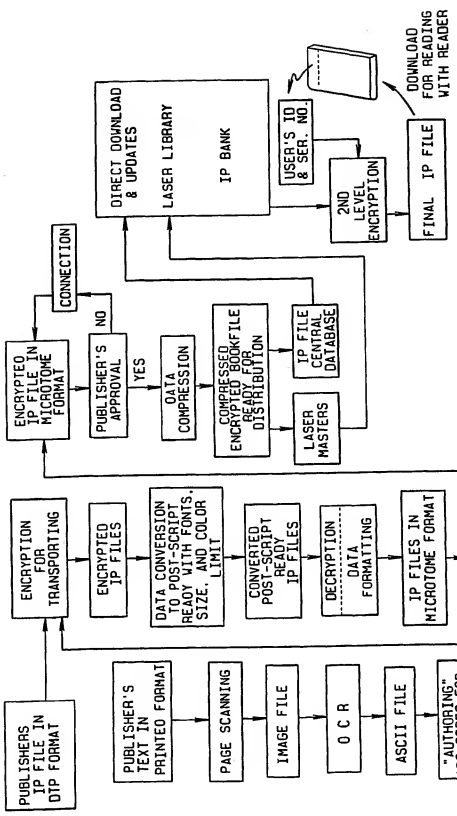


FIG. 12

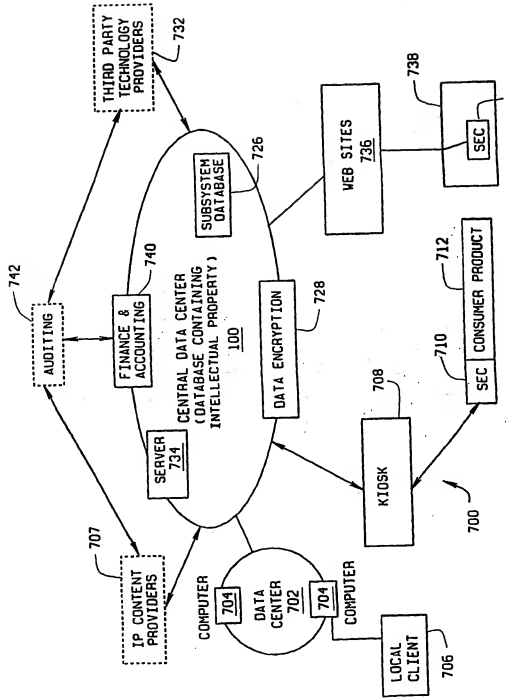


FIG. 14

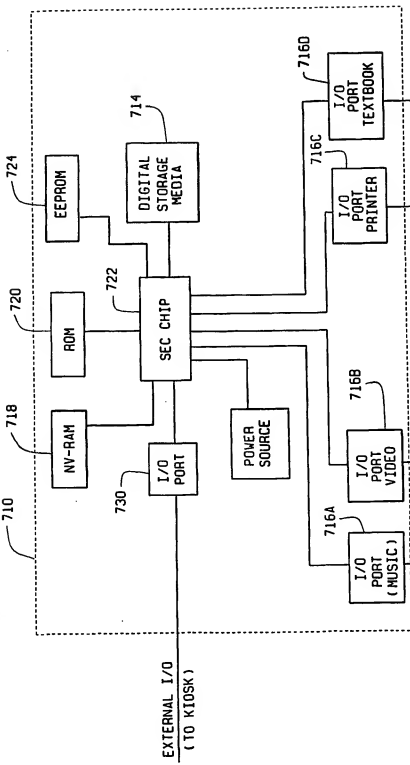


FIG. 15

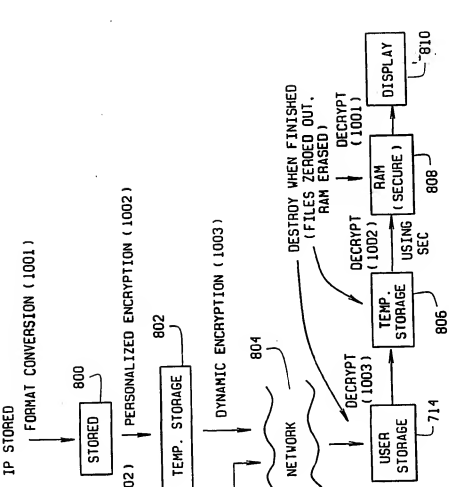


FIG. 16

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/05706

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 17/60
US CL : 705/50

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 705/50, 51, 52, 53, 54, 57

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,910,987 A (GINTER et al) 08 June 1999 (08.06.1999), See entire document	1-92
A	US 5,715,403 A (STEFIK) 03 February 1998 (03.02.1998), See entire document	1-92
A	US 5,388,196 A (PAJAK et al) 07 February 1995 (07.02.1995), See entire document	1-92
A	US 4,855,725 A (FERNANDEZ) 08 August 1989 (08.08.1989), See entire document	1-92
A	US 4,899,292 A (MONTAGNA et al) 06 February 1990 (06.02.1990), See entire document	1-92

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
24 May 2001 (24.05.2001)

Date of mailing of the international search report
18 JUN 2001

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703)305-3230

Authorized officer
James Trammell
Telephone No. (703)305-9700

Form PCT/ISA/210 (second sheet) (July 1998)